ESCUELA SUPERIOR DE INGENIERÍA

GRADO EN INGENIERÍA INFORMÁTICA

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

AUTOR: CARLOS CARRETERO AGUILAR

Cádiz, julio 2017

ESCUELA SUPERIOR DE INGENIERÍA

GRADO EN INGENIERÍA INFORMÁTICA

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

DIRECTOR: CARLOS RODRÍGUEZ CORDÓN
AUTOR: CARLOS CARRETERO AGUILAR

Cádiz, julio 2017

Agradecimientos

A Carlos, por su inestimable predisposición a ayudar en todo lo posible.

A Manolo, por sus inagotables ganas de ayudarme en mi desarrollo profesional.

A mis padres, por darme la oportunidad de crecer como persona y convertirme en quién soy.

A las tres mujeres más bonitas del mundo, por darme todo su amor.

A todos mis compañeros de la universidad, por ayudarme a crecer como persona.

A todos los que han participado de alguna manera u otra, gracias.

Índice de contenido

Índice de figuras

Índice de tablas

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

REF: 0000001

MEMORIA

CLIENTE: EMPRESA PROVINCIAL DE INFORMACIÓN DE CÁDIZ S.A. (EPICSA)
PLAZA MADRID S/N, EDIFICIO CARRANZA, FONDO SUR, LOCAL 10, 11010 CÁDIZ
956261500

AUTOR: CARLOS CARRETERO AGUILAR
INGENIERO INFORMÁTICO
25603515-F
CARLOS.CARRETEROAGUILAR@ALUM.UCA.ES

FIRMADO:
SOLICITANTE AUTOR

CÁDIZ, A 1 DE JULIO DE 2017

1 Objeto

El objetivo de este proyecto es implantar en la red interna de la Diputación Provincial de Cádiz un sistema de Información de Seguridad y Administración de Eventos (SIEM) que se constituya principalmente de un sistema de detección de intrusos (IDS) y de un sistema de análisis de vulnerabilidades, con el fin de proveer al administrador de red de herramientas de detección, prevención y análisis de ataques, intrusiones y vulnerabilidades.

El sistema final implementado debe ser capaz de notificar al administrador de red cuándo detecte tráfico indicativo de un intento de intrusión y debe ser capaz, en la medida de lo posible, de tomar medidas paliativas para la detención del intento de intrusión. El sistema también debe ofrecer, mediante informes de detección de vulnerabilidades, la información necesaria para mantener la red lo más segura posible y correlacionar las alertas de intentos de intrusión con las vulnerabilidades detectadas en los equipos activos de la red.

2 Antecedentes

2.1 Estado actual de la entidad

La **Empresa Provincial de Información de Cádiz S.A** (EPICSA) es una empresa pública creada por la Diputación de Cádiz en el año 1984. La creación de EPICSA tiene como objeto la prestación de servicio técnico integral, formación, comercialización y desarrollo e implantación de aplicaciones informáticas, tanto a la propia diputación como a los municipios de menos de 20.00 habitantes de la provincia de Cádiz.

La empresa se sitúa en la ciudad de Cádiz, Plaza Madrid s/n, Edificio Estadio Carranza, Fondo Sur. Local 10.

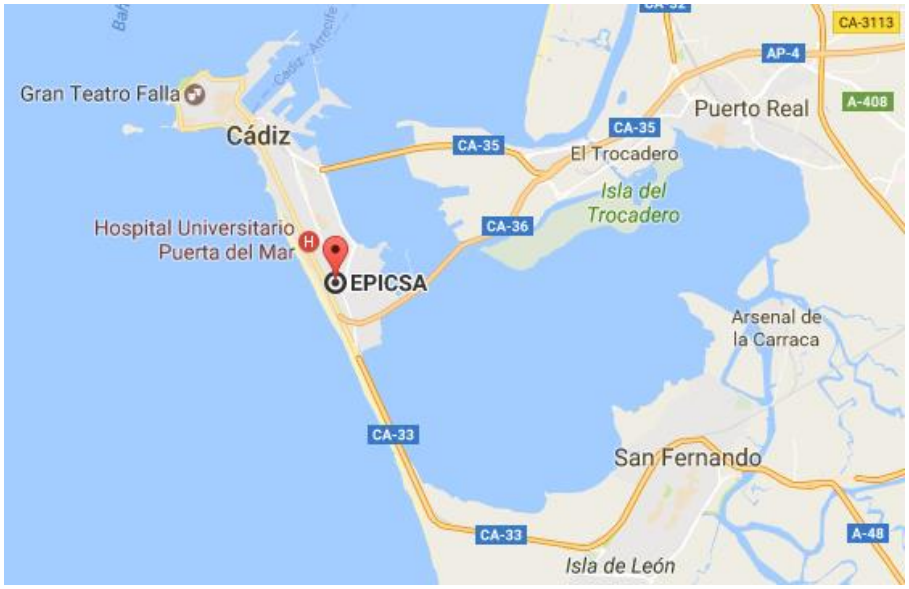


Figura 1 Ubicación de EPICSA en la provincia de Cádiz

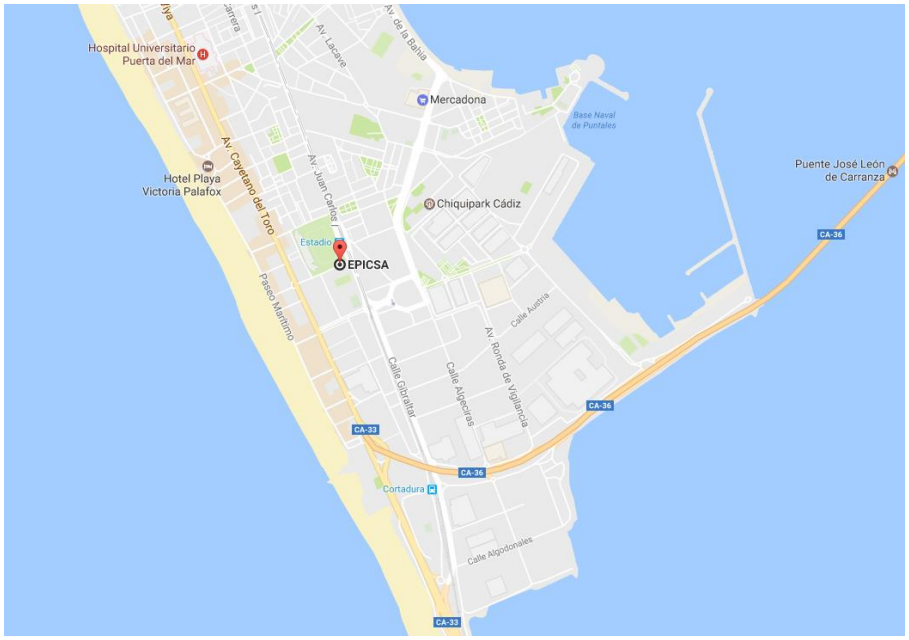


Figura 2 Ubicación de EPICSA en la ciudad de Cádiz

EPICSA centra su actividad en garantizar el correcto funcionamiento de todas las aplicaciones corporativas y de las redes de datos que pertenezcan al dominio establecido de sus competencias a nivel provincial.

EPICSA ofrece un amplio catálogo de servicios a todos los organismos provinciales a los que presta servicio con el fin de hacer realidad una administración electrónica que permita a la ciudadanía y al personal de administración una mayor agilidad, eficiencia y eficacia a la hora de realizar sus tareas cotidianas. Entre los más de 150 trámites incluidos en el amplio catálogo de servicios de administración electrónica se incluyen:

- Gestión de compras y contratación.
- Gestión de Tributos, Ingresos y Recaudación.
- Digitalización de documentos.
- Gestión de decretos.
- Gestión de noticias de prensa.
- Gestión de expedientes de asesoría jurídica.
- Sistema de reserva y alquiler de instalaciones deportivas.
- Gestión de asistencia de empleados y vacaciones.
- Gestión de historias clínicas de pacientes con dependencias.
- Gestión de planes de actuaciones.
- Gestión del registro de licitadores.

Debido a la importancia que tiene la reutilización del software desarrollado, la empresa utiliza software libre (Java) para el desarrollo de sus aplicaciones, así como tecnologías como Struts e Hibernate. Debido a la existencia de aplicaciones que prestan servicio a la gestión tributaria que manejan una gran cantidad de registros y al existir condiciones de seguridad muy restrictivas con el objetivo de cumplir la LOPD, la base de datos utilizada en la empresa es la proporcionada por ORACLE.

También cabe destacar el desarrollo de aplicaciones que la empresa lleva a cabo, como por ejemplo, una aplicación desarrollada conjuntamente con la Escuela para la Prevención de la Violencia para ayudar a las mujeres víctimas de la violencia de género: *EPV-Dipucádiz: Control de Situaciones de Riesgo*.

El organigrama de EPICSA se refleja la figura siguiente:

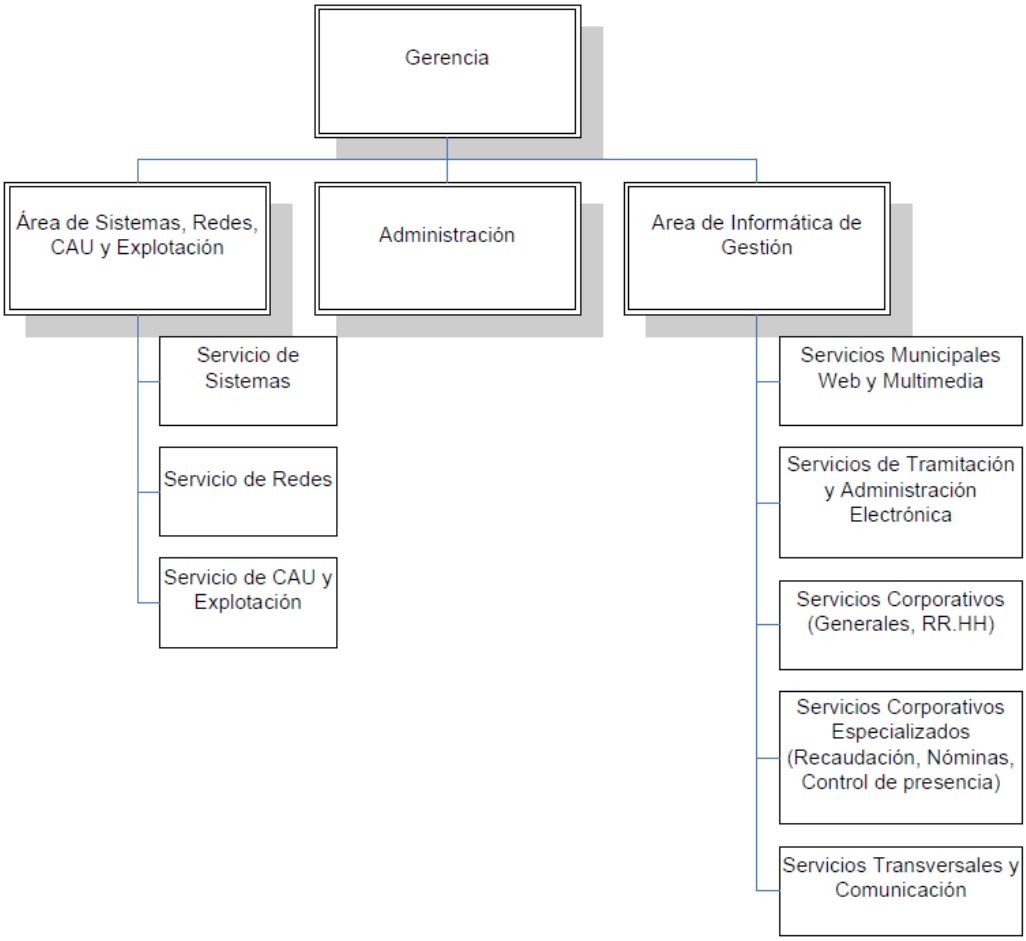


Figura 3 Organigrama de EPICSA

Entre las instalaciones de las que dispone EPICSA, se encuentran un centro de procesamiento de datos (CPD), una planta dedicada al área de sistemas, redes, CAU y explotación, una planta para Administración y para el área de informática de gestión, aulas de formación y un taller de reparación de equipos.

Figura 4 Sala del CPD

Figura 5 Planta del área de sistemas, redes, CAU y explotación

Figura 6 Planta de administración

Entre los municipios de la provincia de Cádiz que cuentan con menos de 20.000 habitantes, se encuentran: Chipiona, Tarifa, Ubrique, Vejer de la Frontera, Villamartín, Medina-Sidonia, Jimena de la Frontera, Olvera, Bornos, Puerto Serrano, Trebujena y Algodonales, entre muchos otros.

Todos los servicios que proporciona EPICSA, ya sean aplicaciones propias o servicios de la Diputación de Cádiz, así como el almacenamiento y la gestión de la mayoría de los datos de la Diputación de Cádiz residen en el Centro de Procesamiento de Datos (CPD) mencionado con anterioridad, con sede en EPICSA.

2.2 Esquema Nacional de Seguridad

En el ámbito de las Administraciones públicas, como la Diputación Provincial de Cádiz, se debe asegurar un desarrollo efectivo y óptimo en la explotación de todos sus servicios electrónicos. Para asegurar esto, se deben incorporar los detalles que aseguran una implantación segura de todas las tecnologías electrónicas. La incorporación de dichos detalles es responsabilidad del Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, del 8 de enero, cuyo objeto es la creación de las condiciones necesarias que aseguren un determinado nivel de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permitan a las Administraciones públicas y a los ciudadanos el normal desarrollo de sus funciones. La fuerte interconexión y dependencia de los datos que existe entre todas las Administraciones públicas y las empresas privadas pone en evidencia que no sólo hay que asegurar la seguridad e integridad de cada sistema de información en particular, si no que hay que asegurar el sistema de enfoque global. Para ello, se debe establecer de manera clara e inequívoca el perímetro y el dominio de seguridad de cada sistema, así como coordinar efectivamente la implantación de todas las medidas de seguridad para evitar fracturas que puedan dañar la información. El

Esquema Nacional de Seguridad provee de las herramientas necesarias para la actuación englobada en materias de seguridad de todas las Administraciones Públicas.

Dentro de las medidas de seguridad que el ENS detalla en su descripción, se incluyen:

- **Medidas que se incluyen en el marco organizativo**. Estas medidas buscan asegurar una evaluación constante y un análisis de la respuesta a los incidentes de forma que se aprenda de la experiencia, se corrijan defectos y/o debilidades y se consiga la excelencia por medio de la mejora continua, alineando este proceso con todas las medidas de seguridad necesarias: políticas de seguridad, normativas de seguridad, etc.
- **Medidas que se incluyen en el marco operacional**. Estas medidas buscan proteger la operación del sistema como conjunto integral de componentes para un fin. Por ejemplo: control de acceso, medidas de aseguramiento de la explotación, monitorización del sistema, etc.
- **Medidas de protección**. Estas medidas de carácter general se aplican con el fin de asegurar la confidencialidad, la integridad y la disponibilidad de los sistemas de información de las Administraciones públicas. Por ejemplo: protección de las instalaciones e infraestructuras, gestión del personal, protección de los equipos, protección de las comunicaciones, etc.

Específicamente, el ENS establece medidas en el marco operacional que se centran en la monitorización de la red corporativa de las Administraciones públicas. La monitorización del sistema permite detectar ataques, e incidentes en general, y habilitar las medidas de reacción necesarias, recopilando la información necesaria para el posterior análisis del incidente. Dentro de la monitorización del sistema de información, el EDS especifica y desarrolla la implantación de un sistema de detección de intrusiones (IDS) que detectará e identificará todo aquello que suponga un uso no autorizado o sospechoso de los sistemas, por ejemplo: descargas masivas de información, escaneo de puertos, descargas de servidores externos, etc.

Dentro de las medidas de protección, el ENS especifica un método de prevención de protección de la información y de los sistemas que consiste en el análisis periódico de las vulnerabilidades de todos los sistemas de información. Dicho análisis consta de tres fases:

1. Revisión exhaustiva de los componentes software.
2. Análisis de vulnerabilidades y estimación del impacto que supondría un incidente.
3. Pruebas de penetración para determinar la posibilidad de explotación de las vulnerabilidades encontradas.

Todas estas descripciones y especificaciones que el ENS desarrolla en su documentación proporcionan un marco de referencia donde se desarrollará este proyecto, especializándose en la implantación de un sistema de detección de intrusiones y un sistema de análisis de vulnerabilidades, ambos integrados en un sistema de información de seguridad y administración de eventos, que cumplan con las especificaciones del ENS.

3 Descripción de la situación actual

La Diputación Provincial de Cádiz dispone de una Red Corporativa Provincial de telecomunicaciones, suministrada por Telefónica, que proporciona servicio de datos y voz a todas las dependencias de la Diputación, sus organismos autónomos y entidades locales a los que da servicio.

3.1 Arquitectura global

La arquitectura global de la Red Corporativa Provincial de telecomunicaciones de la Diputación Provincial de Cádiz es la siguiente:

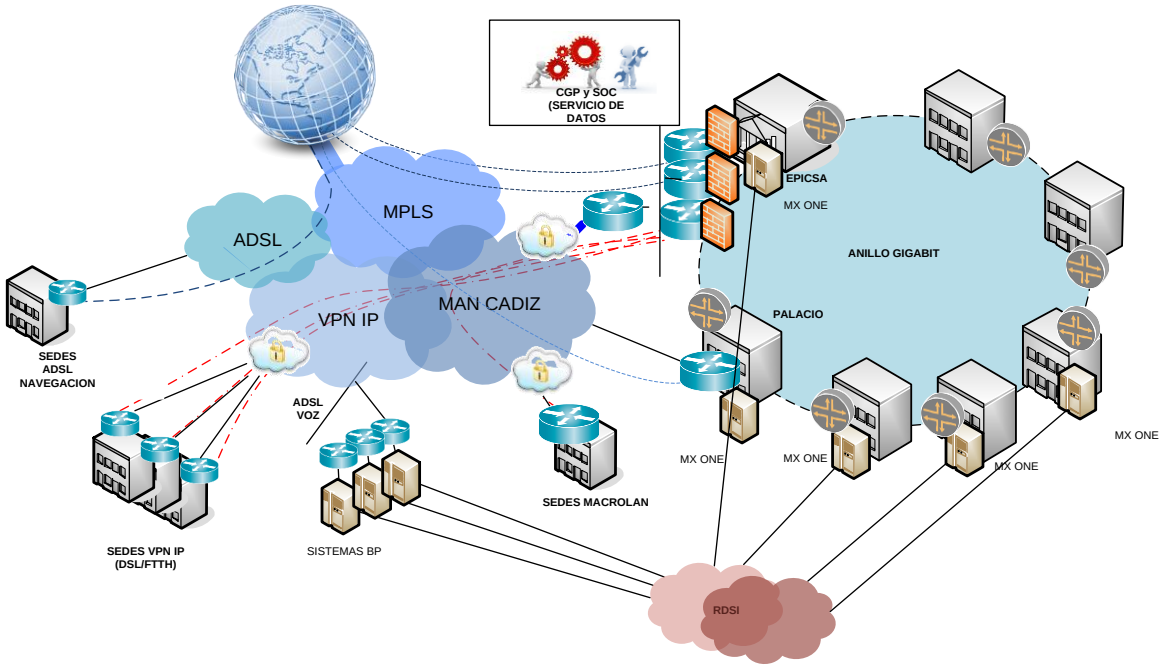


Figura 7 Red de la Diputación Provincial de Cádiz

Para la red de datos metropolitana se ha desplegado un anillo de fibra óptica con ancho de banda de 1 Gbps. Dicho anillo de fibra óptica interconecta todas las sedes de la Diputación Provincial de Cádiz con situación en la propia ciudad de Cádiz.

Para conectar las sedes de la Diputación Provincial de Cádiz externas al anillo metropolitano se ha desplegado una Red Privada Virtual (VPN) que, mediante la tecnología VPN IP de Telefónica, se conectarán dichas sedes remotas a la sede principal ubicada en EPICSA.

El acceso a Internet de la red de la Diputación Provincial de Cádiz se separa en dos tipos de accesos:

- **Internet para publicar.** Este acceso se reserva para el acceso a aplicaciones y servicios propios de la Diputación Provincial de Cádiz. Dicho acceso se soporta sobre un acceso MacroLan de fibra óptica situado en EPICSA.
- **Internet para navegar.** Este acceso se utiliza para el resto de conexiones a Internet. Para las sedes del anillo de red metropolitano se ofrecen dos caudales de

navegación sobre MacroLan de fibra óptica en las sedes de EPICSA y Palacio Provincial. Para las sedes remotas se provee acceso a Internet a través de tecnología DSL.

En lo referente a la seguridad de la red de la Diputación Provincial de Cádiz, se dispone de:

- **Protección de los servicios de publicación.** En la sede de EPICSA, se despliega un clúster de dos Fortigate 600C que realizan la función de cortafuegos.
- **Protección del servicio de navegación para la red metropolitana.** En la sede de EPICSA, se despliega un clúster de dos Fortigate 880C Bundle, que realizan las funciones de cortafuegos, antivirus web y filtrados de URL.
- **Protección del servicio de navegación para oficinas remotas.** Se dispone de un servicio Cloud de navegación segura en modalidad esencial para 480 usuarios nominales con administración delegada en el cliente.

3.2 Modularización de la red

Según el planteamiento teórico que CISCO realiza sobre el diseño funcional de una red, esta se puede dividir en diferentes áreas funcionales que, a su vez, se dividen en diferentes módulos. Si aplicamos la aproximación del diseño funcional de una red al diseño de la red de la Diputación de Cádiz, las áreas funcionales quedan distribuidas de la siguiente manera:

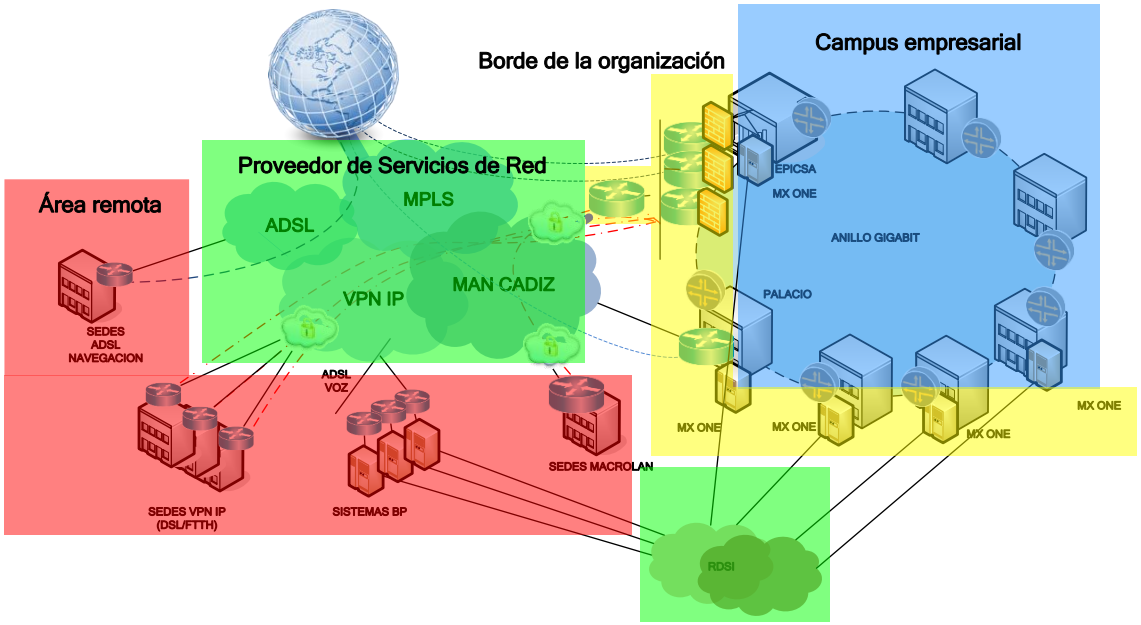


Figura 8 Modularización de la red de la Diputación de Cádiz

3.3 Campus empresarial

Según el diseño funcional propuesto por CISCO, el área del campus empresarial es la sede principal de una organización y, a su vez, se divide en el módulo de infraestructura de red y en el módulo de centro de procesamiento de datos y granja de servidores.

En lo referente a la infraestructura de red, la Diputación Provincial de Cádiz dispone de una red metropolitana en anillo que interconecta las diferentes sedes de la diputación de Cádiz con residencia en la ciudad de Cádiz. Cada una de las sedes de las que dispone la Diputación Provincial de Cádiz corresponde a un nodo de la red metropolitana en anillo, salvo algunas que, por cercanía a otras sedes, se disponen como conexiones directas a otras sedes y no pertenecen al anillo propiamente dicho. Las sedes de la Diputación que pertenecen al área metropolitana son:

SEDE	DOMICILIO	NODO DEL ANILLO
EPICSA	Edf. Carranza – Fondo Sur	EPICSA
Patronato Turismo	Edf. Carranza – Fondo Sur	EPICSA
Mancomunidad	Edf. Carranza – Fondo Sur	EPICSA
Edificio Glorieta	Plaza Zona Franca s/n	GLORIETA
Patronato Vivienda	Plaza Zona Franca s/n	GLORIETA
SPRyGT oficinas centrales	Edificio Europa	EUROPA
Escuela de hostelería	Edificio Europa	EUROPA
Campo del Sur	Campo del Sur, 28	CAMPO DEL SUR
MediaMB	Campo del Sur, 26	CAMPO DEL SUR
Edificio Roma	Av. Ramón de Carranza s/n	ROMA
Palacio Provincial	Plaza España s/n	PALACIO
Edificio Cámara de Comercio	Antonio López 4	ANT LOPEZ
Fundación Provincial de Cultura	Edf. Rivadavia	RIVADAVIA
Edificio San Antonio	Plaza San Antonio s/n	SAN ANTONIO
Instituto de Empleo y Desarrollo Tecnológico	Benito Pérez Galdós, 8	IEDT
Sede Central del SPD	Plaza de Capuchinos, 3	CAPUCHINOS
C.T.A. de Cádiz	Avda. Guadalquivir, s/n	GUADALQUIVIR
Residencia Provincial "José María Calvo"	C/ Dr. Marañón 5	RESIDENCIA

Tabla 1 Sedes de la Diputación Provincial de Cádiz en la ciudad de Cádiz

Tanto la sede Patronato Turismo como la sede Mancomunidad son sedes a todos los efectos, pero no pertenecen al anillo propiamente dicho, sino que se conectan de manera interna al nodo del anillo de EPICSA, ya que las tres sedes residen en el mismo edificio. La sede MediaMB, por cercanía con la sede Campo del Sur, se ha dispuesto como enlace interno directo a dicha sede, por lo que tampoco pertenece al anillo propiamente dicho. Lo mismo ocurre con la sede Patronato Vivienda, que por cercanía se conecta con el nodo del anillo Glorieta. La escuela de hostelería también está conectada al nodo del anillo de la sede Europa. La disposición de la red de anillo metropolitana es la siguiente:

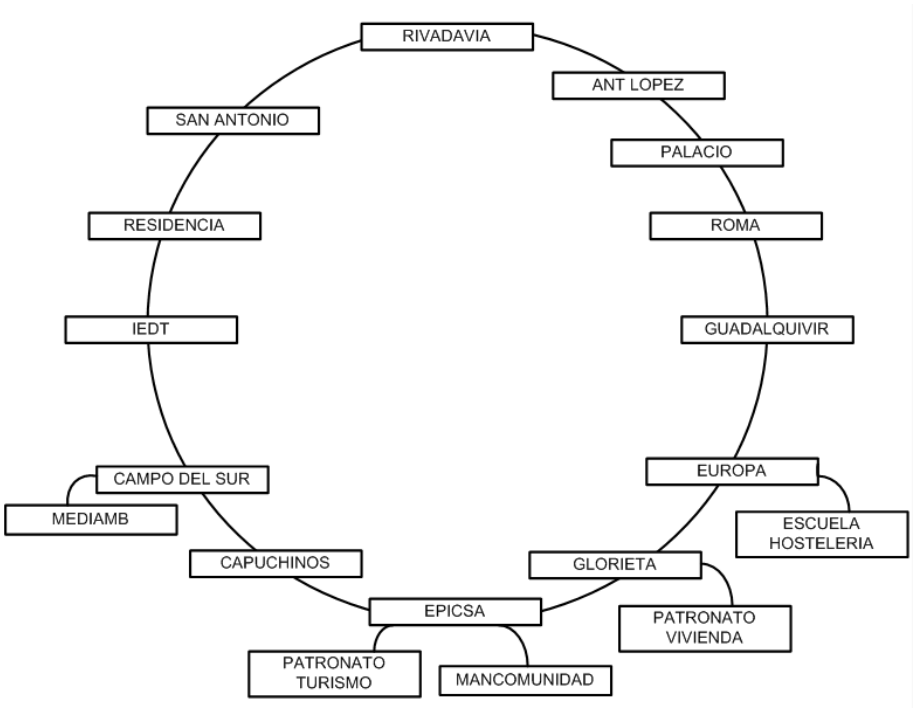


Figura 9 Sedes de la Diputación en el anillo metropolitano

En la siguiente ilustración se muestra de manera gráfica la disposición del anillo en la ciudad de Cádiz de manera aproximada. Todas las sedes que están directamente conectadas a sedes del anillo se han omitido debido a que comparten la misma localización.

Figura 10 Distribución geográfica aproximada del anillo metropolitano

Las conexiones entre los nodos de la red, que representan a cada una de las sedes de la Diputación dentro de la ciudad de Cádiz, se realizan mediante fibra óptica monomodo

sobre la que hay implementada una tecnología Ethernet 1000baseLX con ancho de banda de 1 Gbps. Cada uno de los nodos de la red dispone de cuatro cables de fibra óptica que los unen al anillo, un par de cables vienen de una sede y el otro par de cables van a la sede siguiente del anillo.

Al final, la Diputación Provincial de Cádiz dispone de una red de anillo metropolitana que interconecta sedes separadas geográficamente que se comporta como una LAN única, que proporciona conectividad de alta disponibilidad y alta redundancia ante fallos a todas las sedes que se interconectan al anillo.

3.3.1 Electrónica de red

En este apartado se describen toda la electrónica de red que se utiliza en la red de EPICSA S.A. La ubicación específica de cada equipo que conforma la red se especificará en el apartado siguiente, dónde se describe la topología específica de cada sede de la Diputación Provincial de Cádiz

3.3.1.1 HI 5500-24G-4SFP JG311A

Para la interconexión de los diferentes nodos del anillo metropolitano, se han desplegado conmutadores de capa 3 de la marca Hewlett-Packard (HP), modelo HI 5500-24G-4SFP JG311A.

Figura 11 Conmutador HP HI 5500-24G-4SFP JG311A

Las características principales del conmutador HP HI 5500-24G-4SFP JG311A son las siguientes:

Concepto	Valor
Fabricante	HP
Enrackable	Sí
Puertos	24 Ethernet 10/100/1000 Mbps 4 SFP 1GbE 2 SFP+ 10GbE 2 expansión
Espacio en Us	1
Capacidad	224 Gbps
Throughput	166,6 Mbps
Nº máximo puertos 1G	64
Nº máximo puertos 10G	6
Nº máximo de fuentes de alimentación	2
Puertos de gestión	RS232 + OOB
Autenticación	DB local, RADIUS y TACACS+

Soporte 802.1q	Sí
Nº máximo de VLANs	1024
Protocolos de enrutamiento	RIP(v2), OSPF(v3), ISIS, BGP
Soporte de clustering	Sí, mediante IRF. Máximo: 9 u/clúster

Tabla 2 Especificaciones conmutador HP HI 5500-24G-4SFP JG311A

El diseño de la red dispone que la conexión de cada nodo con el anillo de fibra se realiza con un clúster de conmutadores HP HI 5500-24G-4SFP, de modo que cada uno de los nodos dispone en la capa de núcleo de dos conmutadores HP que, a efectos lógicos, funcionan como un solo punto de conexión con el anillo.

El agrupamiento lógico de los conmutadores HP se realiza mediante la tecnología de HP denominada Intelligent Relisilient Framework (IRF). Esta tecnología permite que dos conmutadores HP diferentes funcionen como un solo conmutador virtual. El conmutador virtual se comporta como un único equipo en nivel de capa 2, en nivel de capa 3 y a nivel de gestión. La interconexión de los dos conmutadores físicos se realiza mediante enlaces de 10 GbE, de manera que los conmutadores que conforman la agrupación virtual se pueden distribuir geográficamente.

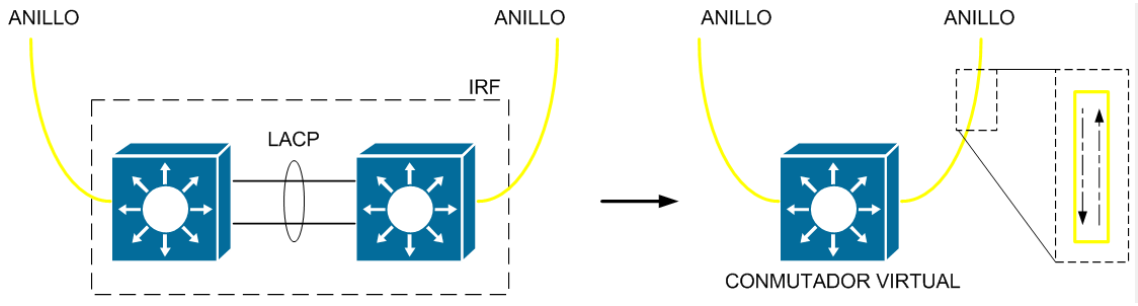


Figura 12 Funcionamiento de IRF

Dado que dos conmutadores diferentes se agrupan en uno virtual, permite que se utilice agregado LACP (802.3ad) en los enlaces redundantes. LACP (Protocolo de Control de Agregación de Enlaces) es un protocolo que permite agrupar de manera lógica diferentes enlaces iguales conectados entre dos mismos equipos, provocando un aumento del ancho de banda y un balanceo de carga entre los diferentes enlaces físicos, que funcionan como un solo enlace lógico.

3.3.1.2 HP 5120-48G EI JE067A

Para el proporcionar el acceso a la red a los usuarios en algunas de las sedes de la Diputación Provincial de Cádiz se utiliza un conmutador HP, modelo 5120-48G EI JE067A

Figura 13 Conmutador HP 5120-48G EI JE067A

Las características principales del conmutador HP 5120-48G EI JE067A son las siguientes:

Concepto	Valor
Fabricante	HP
Enrackable	Sí
Puertos	44 Ethernet 10/100/1000 Mbps 4 Personales-duales 10/100/1000 o SFP
Espacio en Us	1
Capacidad	96 Gbps
Throughput	47,98 Mbps
Nº máximo de fuentes de alimentación	1
Puertos de gestión	RS232
Soporte 802.1q	Sí
Nº máximo de VLANs	1024

Tabla 3 Especificaciones conmutador HP 5120-48G EI JE067A

3.3.1.3 3COM Baseline Switch 2928 SFP Plus 3CRBSG2893

Para el acceso de los usuarios a la red de la Diputación Provincial de Cádiz en la sedes IEDT, Europa y en la escuela de hostelería se utiliza un conmutador 3COM, modelo Baseline Switch 2928 SFP Plus 3CRBSG2893.

Figura 14 Conmutador 3COM Baseline Switch 2928 SFP Plus 3CRBSG2893

Las características principales del conmutador 3COM Baseline Switch 2928 SFP Plus 3CRBSG2893 son las siguientes:

Concepto	Valor
Fabricante	3COM
Enrackable	Sí
Puertos	24 Ethernet 10/100/1000 Mbps 4 SFP 1000 Mbps
Espacio en Us	1
Capacidad	56 Gbps
Throughput	41,7 Mbps
Nº máximo de fuentes de alimentación	1
Puertos de gestión	RS232
Soporte 802.1q	Sí
Nº máximo de VLANs	1024

Tabla 4 Especificaciones 3COM Baseline Switch 2928 SFP Plus 3CRBSG2893

3.3.1.4 3COM Baseline Switch 2924 SFP Plus 3CBLSG24-ME

Para el acceso de los usuarios a la red de la Diputación Provincial de Cádiz en la sedes IEDT y Roma, se utiliza un conmutador 3COM, modelo Baseline Switch 2924 SFP Plus 3CBLSG24-ME

Figura 15 Conmutador 3COM Baseline Switch 2924 SFP Plus 3CBLSG24-ME

Las características principales del conmutador 3COM Baseline Switch 2924 SFP Plus 3CBLSG24-ME son las siguientes:

Concepto	Valor
Fabricante	3COM
Enrackable	Sí
Puertos	24 Ethernet 10/100/1000 Mbps 4 SFP 1000 Mbps
Espacio en Us	1
Capacidad	48 Gbps
Throughput	35,5 Mbps
Nº máximo de fuentes de alimentación	1
Puertos de gestión	RS232
Soporte 802.1q	Sí
Nº máximo de VLANs	1024

Tabla 5 Especificaciones 3COM Baseline Switch 2924 SFP Plus 3CBLSG24-ME

3.3.1.5 CISCO WS-C3550-48-EMI

Para el acceso de los usuarios a la red de la Diputación Provincial de Cádiz en la sede IEDT, se utiliza un conmutador CISCO, modelo WS C3550-48 EMI

Figura 16 Conmutador CISCO WS C3550-48 EMI

Las características principales del conmutador CISCO WS C3550-48 EMI son las siguientes:

Concepto	Valor
Fabricante	CISCO
Enrackable	Sí
Puertos	48 Ethernet 10/100 Mbps 2 1000BASE-X

Espacio en Us	1
Capacidad	13,6 Gbps
Throughput	10,1 Mbps
Nº máximo de fuentes de alimentación	1
Puertos de gestión	RS232
Soporte 802.1q	Sí
Nº máximo de VLANs	1024

Tabla 6 Especificaciones conmutador CISCO WS C3550-48 EMI

3.3.1.6 HP A3100-24 EI JD320B

Para el acceso de los usuarios a la red de la Diputación Provincial de Cádiz en la sede Antonio Lopez, se utiliza un conmutador HP, modelo A3100-24 EI JD320B

Figura 17 Conmutador HP A3100-24 EI JD320B

Las características principales del conmutador HP A3100-24 EI JD320B son las siguientes:

Concepto	Valor
Fabricante	HP
Enrackable	Sí
Puertos	14 Ethernet 10/100 Mbps 2 Personales-duales 10/100/1000 o SFP
Espacio en Us	1
Capacidad	8,8 Gbps
Throughput	5,91 Mbps
Nº máximo de fuentes de alimentación	1
Puertos de gestión	RS232
Soporte 802.1q	Sí
Nº máximo de VLANs	1024

Tabla 7 Especificaciones conmutador HP A3100-24 EI JD320B

3.3.2 Plan de direccionamiento

La red en anillo metropolitana de la Diputación Provincial de Cádiz tiene clasificadas las direcciones IP en cuatro grupos:

- **Gestión**, cuyas direcciones IP pertenecen a la VLAN 1. Estas direcciones se utilizan para administrar todos los conmutadores de la red.
- **Servidores**, cuyas direcciones IP pertenecen a la VLAN 3. Estas direcciones se utilizan para configurar los servidores de EPICSA.
- **Fortigate**, cuyas direcciones IP pertenecen a la VLAN 15. Estas direcciones se utilizan para configurar los firewalls de EPICSA que hacen de frontera con Internet.
- **Transporte**, cuyas direcciones IP pertenecen a la VLAN 50. Estas direcciones se utilizan para configurar los enlaces directos de fibra del anillo.

- **Clientes**, cuyas direcciones IP pertenecen desde la VLAN 100 a la 132, según la sede donde se encentren los usuarios de los equipos. Estas direcciones se utilizan para dar acceso a los usuarios a la red de la Diputación.

El plan de direccionamiento es el siguiente:

Sede	Grupo	Rack	VLAN	Red	Puerta de enlace
Todas	Gestión	Todos	1 – default	172.32.1.0/24	172.32.1.1
EPICSA	Servidores	Todos	3 – DIPUTACION	172.22.0.0/19	172.22.5.25
EPICSA	Fortigate	CPD	15 – Fortigate	194.179.87.18/29	x
Todas	Anillo	Principal	50 – TRANSPORTE	10.12.50.0/24	10.12.50.100
EPICSA	Clientes	CPD	100 – EPICSA-Planta-baja	10.12.100.0/24	10.12.100.1
EPICSA	Clientes	Rack 1	101 – EPICSA-Planta-primera	10.12.101.0/24	10.12.101.1
EPICSA	Clientes	CPD	102 – EPICSA-Aula-formacion	10.12.102.0/24	10.12.102.1
EPICSA	Clientes	CPD	103 – EPICSA-Taller	10.12.103.0/24	10.12.103.1
PATRONATO	Clientes	Principal	104 – Patronato	10.12.104.0/24	10.12.104.1
MANCOMUNIDAD	Clientes	Principal	105 – Mancomunidad	10.12.105.0/24	10.12.105.1
CAPUCHINOS	Clientes	Principal	106 – Capuchinos	10.12.106.0/24	10.12.106.1
CAMPO DEL SUR	Clientes	Principal	107 – Agencia-Energia	10.12.107.0/24	10.12.107.1
MEDIAMB	Clientes	Principal	108 – MediaMB	10.12.108.0/24	10.12.108.1
IEDT	Clientes	Principal	109 – IEDT	10.12.109.0/24	10.12.109.1
RESIDENCIA	Clientes	Principal	110 – Residencia-Mayores	10.12.110.0/24	10.12.110.1
RIVADAVIA	Clientes	Principal	116 – Rivadavia	10.12.116.0/24	10.12.116.1
SAN ANTONIO	Clientes	Principal	117 – San-Antonio	10.12.117.0/24	10.12.117.1
PALACIO	Clientes	Rack 1	120 – Palacio-Rack1	10.12.120.0/24	10.12.118.1
PALACIO	Clientes	Rack 2	121 – Palacio-Rack2	10.12.121.0/24	10.12.119.1
PALACIO	Clientes	Rack 3	122 – Palacio-Rack3	10.12.122.0/24	10.12.124.1
PALACIO	Clientes	Rack 4	123 – Palacio-Rack4	10.12.123.0/24	10.12.125.1
ROMA	Clientes	Rack 1	126 – Roma-Switch1	10.12.126.0/24	10.12.126.1
ROMA	Clientes	Rack 2	128 – Roma-Switch2	10.12.128.0/24	10.12.128.1
GUADALQUIVIR	Clientes	Principal	130 – Avda-Guadalquivir	10.12.130.0/24	10.12.130.1
EUROPA	Clientes	Principal	131 – Europa	10.12.131.0/24	10.12.131.1
GLORIETA	Clientes	Principal	132 – Glorieta	10.12.132.0/24	10.12.132.1
ANT LOPEZ	Clientes	Principal	150 - AntonioLopez	10.12.150.0/24	10.12.150.1

Tabla 8 Plan de direccionamiento de la Diputación Provincial de Cádiz

Las sedes conectadas a Europa y Glorieta pertenecen al espacio de direcciones y a las VLANs asignadas a las sedes Europa y Glorieta, respectivamente. La siguiente ilustración especifica que dirección, dentro de la VLAN 1, del grupo Gestión, tiene cada nodo del anillo metropolitano para su administración.

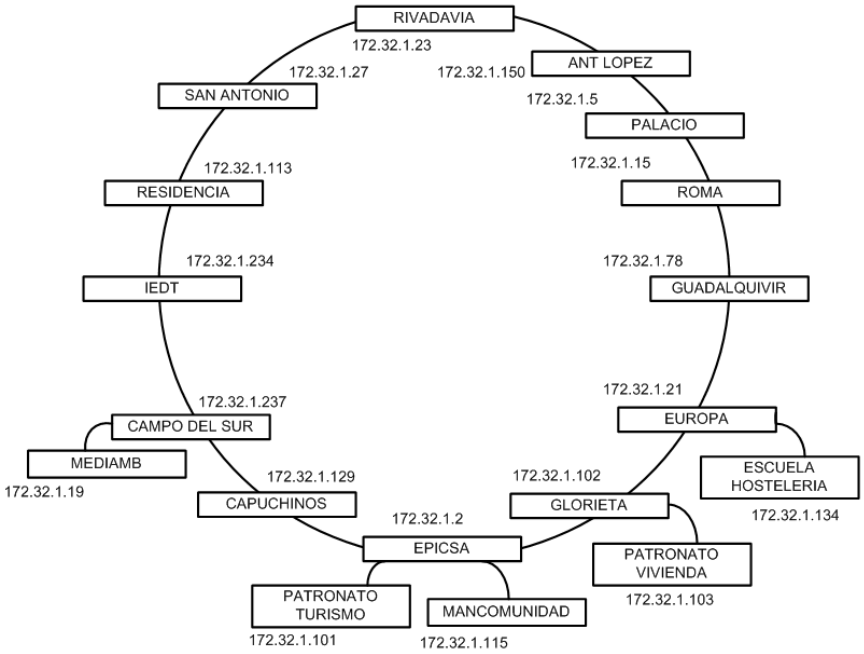


Figura 18 Direcciones de los nodos del anillo

3.3.3 Funcionamiento de la red

Propagación de VLANs

El alcance de cada VLAN configurada es el siguiente:

- VLAN 1 – Gestión. Se propagará a todos los equipos de la red. Sin acceso desde el exterior
- VLAN 3 – Servidores. Se propagará en el CDP de EPICSA.
- VLAN 15 – Fortigate. Solo se propagará a equipos que pertenezcan al anillo.
- VLAN 50 – Transporte. Solo se propagará a equipos del anillo.
- VLAN 100…132 – Clientes. Solo se propagará a la sede a la que dan servicio.

Enrutamiento y asignación de direcciones

El enrutamiento en la red se realiza de manera dinámica utilizando el protocolo de enrutamiento dinámico OSPF para IPv4.

El protocolo OSPF (Open Shortest Path First), es un protocolo de enrutamiento dinámico de interior (IGP), que utiliza algoritmos SPF para calcular la mejor ruta entre dos nodos cualesquiera de un mismo sistema autónomo. Para calcular la mejor ruta a un destino se utiliza una métrica denominada coste, que tiene en cuenta parámetros de la red, como por ejemplo el ancho de banda de las interfaces de red. OSPF construye en cada nodo de la red una base de datos que contiene todos los enlaces existentes en la red y sus estados. Una red OSPF se puede descomponer en pequeños dominios denominados áreas. Todas las áreas deben estar conectadas al área 0, o área backbone. Cabe destacar que pueden existir redes que utilizan el protocolo OSPF dónde solo exista el área 0.

El protocolo OSPF se ha implementado mediante la configuración de una sola área, la 0 (área Backbone), a la que pertenecerán todos los conmutadores de capa núcleo que

pertenecen al anillo de fibra. Se han protegido las comunicaciones del protocolo OSPF con autenticación cifrada mediante MD5. Todos los mensajes de OSPF necesarios para su funcionamiento se transportarán utilizando la VLAN 50.

Para las sedes que no disponen de un conmutador en el anillo, el enrutamiento lo llevará a cabo el conmutador HP del anillo más cercano:

- Sedes Patronato y Mancomunidad: conmutador de EPICSA.
- Sede MediaMB: conmutador de Campo del Sur.

Para todos los equipos pertenecientes a las VLANs del grupo Clientes (100-132), las direcciones IP serán asignadas dinámicamente por parte del conmutador HP de núcleo correspondiente en el anillo mediante DHCP.

El encargado de distribuir las rutas para llegar a todos los ayuntamientos y/o sedes remotas de la Diputación de Cádiz que no pertenecen al anillo es el conmutador de EPICSA que tiene la función de nodo del anillo.

Protocolo Spanning Tree

La estructura de la topología de anillo dispuesta en la red metropolitana de la Diputación Provincial de Cádiz provoca que esta sea susceptible de sufrir bucles en capa 2 debido a enlaces redundantes.

Para solucionar este problema, se desarrolló el protocolo Spanning Tree (STP), IEE 802.1D. En una topología con STP, los conmutadores decidirán que enlaces de la topología se desactivan a fin de evitar los bucles en la red. Lo primero que hacen los conmutadores es elegir un conmutador raíz y un conmutador raíz de respaldo, los cuales servirán de referencia para calcular los costes de llegada a cada una de los segmentos de red existentes en la topología.

Más tarde, cada conmutador debe especificar cuáles de sus puertos es el que tiene menos coste para llegar al conmutador raíz. Una vez que se han elegido los puertos raíz, se han de elegir los puertos designados. Un puerto designado es, en un segmento de red con enlaces entre dos conmutadores, el puerto con menos coste para llegar al conmutador raíz. Cuándo se han elegido los puertos designados, todos aquellos que hayan quedado fuera de la selección deberán bloquearse, para así evitar los bucles. Quedarán como puertos bloqueados.

Si la topología de red cambia, ya sea porque un puerto de un conmutador deja de funcionar o porque se desconecta un cable, hay que realizar todos los cálculos de nuevo, lo que puede llevar bastante tiempo. Para evitar este problema, existe el protocolo Spanning Tree Rápido (RSTP), 802.1w que asegura menores tiempos de convergencia.

Para redes con VLANs configuradas, como la red de la Diputación Provincial de Cádiz, existe una versión de RSTP que lanza una instancia del protocolo para cada VLAN configurada. Esta versión de RSTP se llama protocolo Rapid Per-VLAN Spanning Tree (RPVST).

Para la red de la Diputación Provincial de Cádiz se ha configurado RPVST, con las siguientes instancias:

- Instancia 1: VLANs 1-3, 15, 33, 50, 100-200
- Instancia 2 VLANs 21-23, 23, 40

Al final, el cálculo de conmutadores raíz y puertos bloqueados es el mismo para todas las VLANS y la topología queda de la siguiente manera:

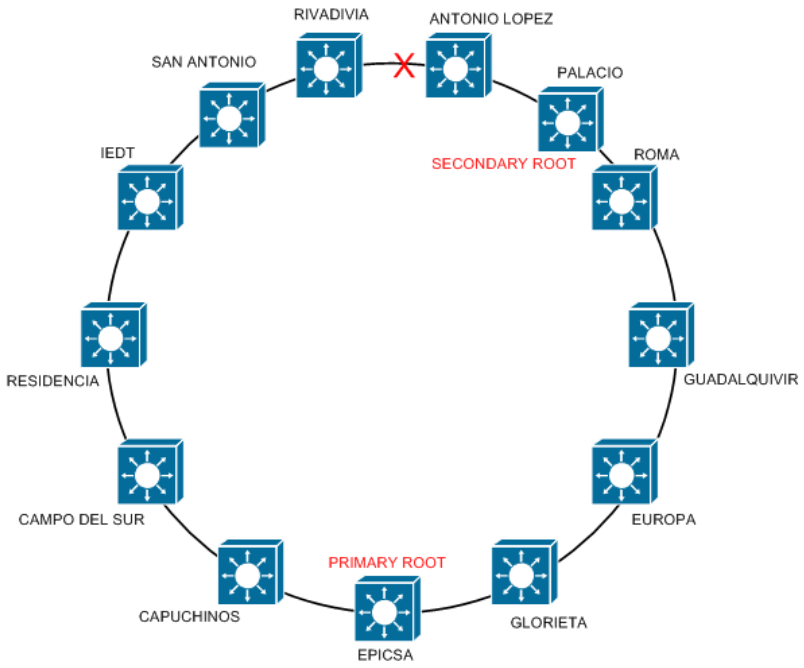


Figura 19 Topología del anillo con protocolo RPVST

3.3.4 Topología de red en las sedes

Cada una de las sedes pertenecientes a la red metropolitana de la Diputación Provincial de Cádiz tiene su propia topología de red para la capa de distribución y para la capa de acceso

3.3.4.1 Sedes EPICSA, Patronato Turismo y Mancomunidad

El nodo del anillo EPICSA, incluye la topología de red de la sede de EPICSA, de la sede Patronato de Turismo y de la sede Mancomunidad. Las sedes de Patronato de Turismo y Mancomunidad se conectan directamente al clúster IRF de conmutadores HP 5500 de capa 3 (SWL3-EPICSA). La topología de red de la sede sigue una arquitectura de dos capas: Núcleo colapsado y acceso. La capa de núcleo colapsado incluye el clúster IRF de conmutadores HP 5500 y existen tres capas de acceso, una por sede.

El esquema de la topología de red es el siguiente:

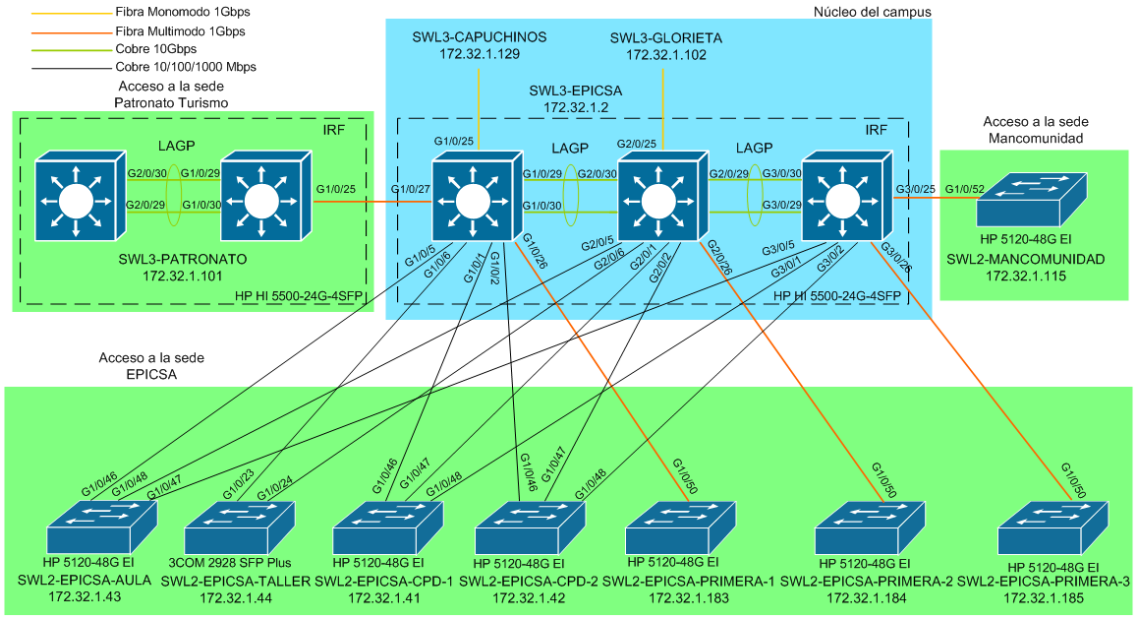


Figura 20 Topología de red de las sedes Epicsa, Patronato Turismo y Mancomunidad

3.3.4.2 Sede Capuchinos

La sede Capuchinos posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-CAPUCHINOS). La capa de núcleo incluye al clúster IRF de HP 5500. Los mismos conmutadores de capa de núcleo realizan las funciones de capa de acceso a la sede Capuchinos.

El esquema de la topología de red es el siguiente:

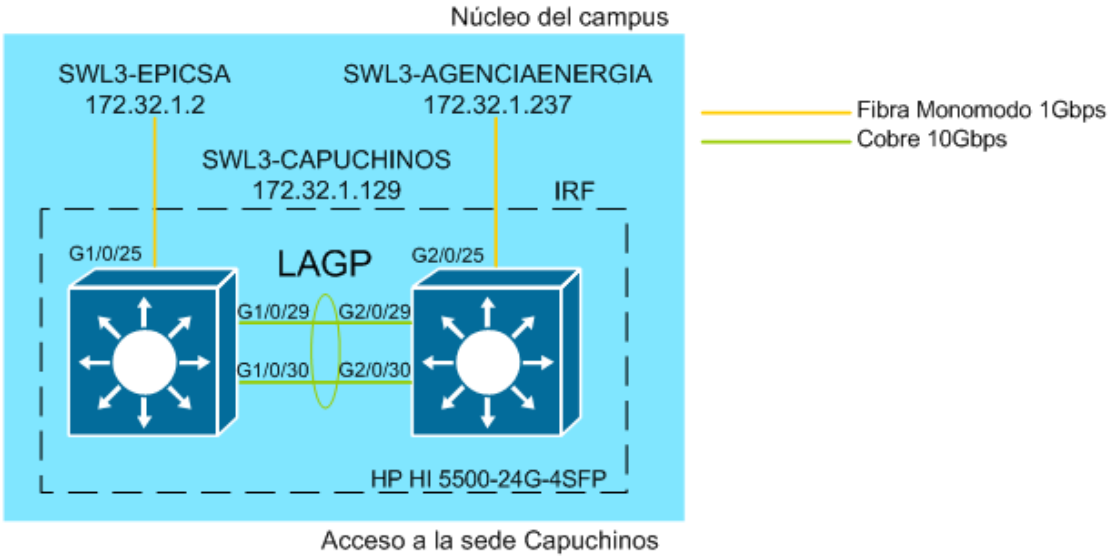


Figura 21 Topología de red de la sede Capuchinos

3.3.4.3 Sedes Campo del Sur y MediaMB

Las sedes Campo del Sur y MediaMB disponen de un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión con el anillo (SWL3-AGENCIAENERGIA). La sede MediaMB se conecta mediante fibra directamente al clúster IRF. La conexión de los usuarios finales se realiza mediante enlaces directos al clúster para la sede Campo del Sur y

enlaces al conmutador SWL2-MEDIAMB para los usuarios de la sede MediaMB. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500. Dicho clúster también realiza las funciones de capa de acceso para la sede Agencia de Energía. El conmutador SLW2-MEDIAMB realiza las funciones de capa de acceso para la sede MediaMB.

El esquema de la topología de red es el siguiente:

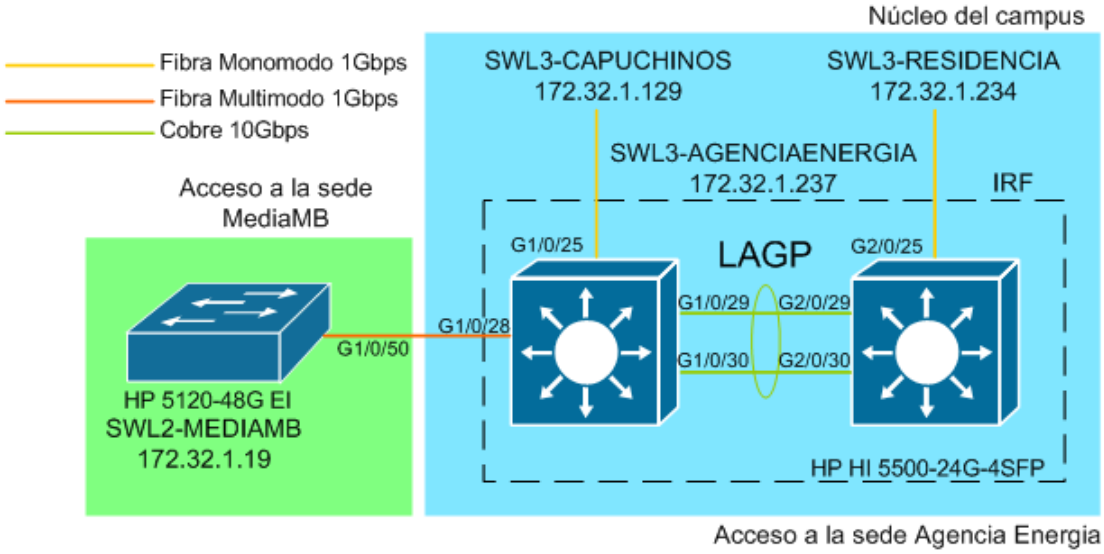


Figura 22 Topología de red de las sedes Campo del Sur y MediaMB

3.3.4.4 Sede IEDT

La sede IEDT dispone de un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-IEDT). La topología de red sigue una arquitectura de dos capas: Núcleo colapsado y acceso. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500. Los conmutadores SWL2-IEDT-REGISTRO, SWL2-IEDT-FOTOVOL y SWL2-IEDT-MULTI-1 realizan las funciones de capa de acceso para la sede IEDT.

El esquema de la topología de red es el siguiente:

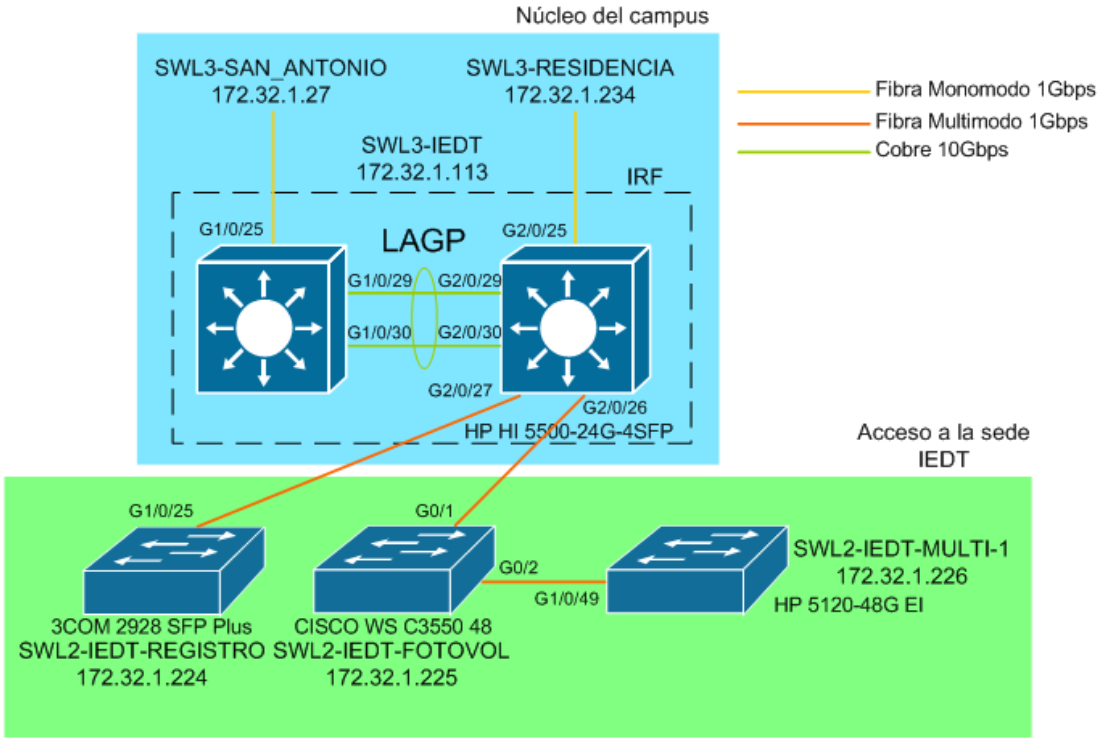


Figura 23 Topología de red de la sede IEDT

3.3.4.5 Sede Residencia

La sede Residencia posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-RESIDENCIA). Debido al escaso número de equipos de clientes finales activos en la sede, la conexión de los usuarios se proporciona con enlaces directos al clúster. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500, siendo el mismo clúster el que realiza las funciones de capa de acceso para la sede Residencia.

El esquema de la topología de red es el siguiente:

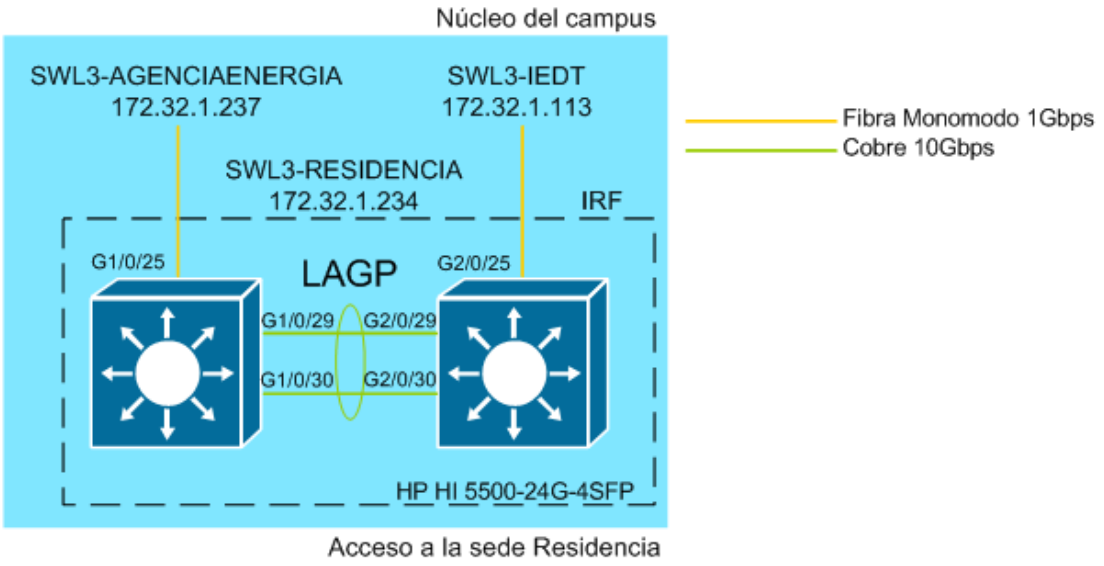


Figura 24 Topología de red de la sede Residencia

3.3.4.6 Sede San Antonio

La sede San Antonio posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-SAN_ANTONIO). Debido al escaso número de equipos de clientes finales activos en la sede, la conexión de los usuarios se proporciona con enlaces directos al clúster. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500, siendo el mismo clúster el que realiza las funciones de capa de acceso para la sede San Antonio.

El esquema de la topología de red es el siguiente:

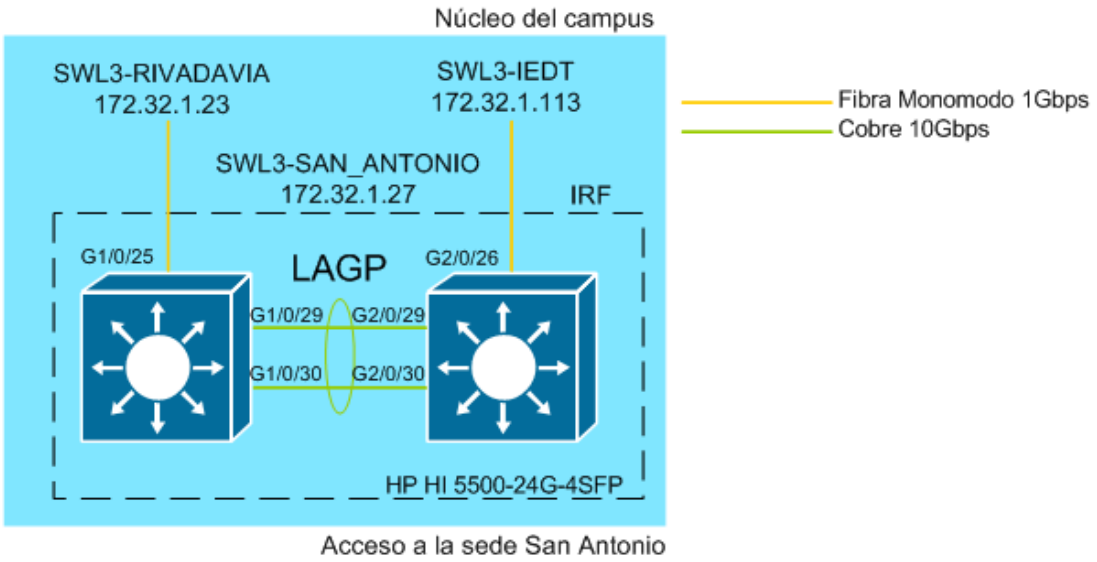


Figura 25 Topología de red de la sede San Antonio

3.3.4.7 Sede Rivadavia

La sede Rivadavia posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-RIVADAVIA). Debido al escaso número de equipos de clientes finales activos en la sede, la conexión de los usuarios se proporciona con enlaces directos al clúster. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500, siendo el mismo clúster el que realiza las funciones de capa de acceso para la sede Rivadavia.

El esquema de la topología de red es el siguiente:

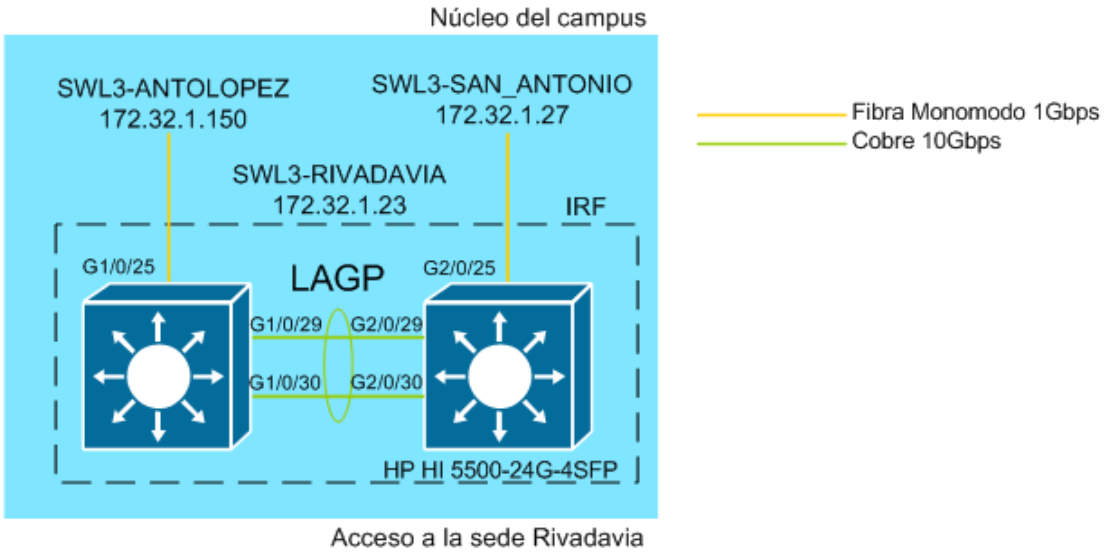


Figura 26 Topología de red de la sede Rivadavia

3.3.4.8 Sede Antonio López

La sede Antonio López posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-ANTOLOPEZ). La topología de red de la sede sigue una arquitectura de dos capas: núcleo colapsado y acceso. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500. Los conmutadores SWL2-ANTOLOPEZ-R[1-3]-[1-3] realizan las funciones de capa de acceso para la sede Antonio López.

El esquema de la topología de red es el siguiente:

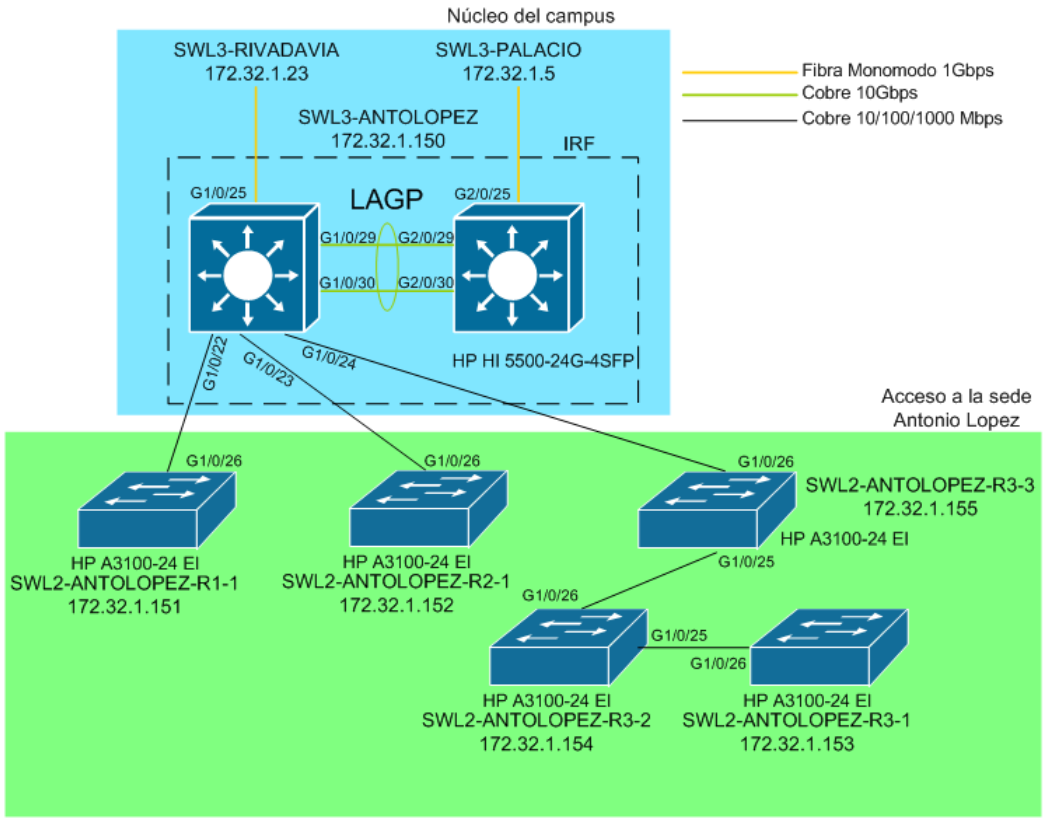


Figura 27 Topología de red de la sede Antonio López

3.3.4.9 Sede Palacio

La sede Palacio posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-PALACIO). La topología de red de la sede sigue una arquitectura de tres capas: núcleo, distribución y acceso. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500. Las funciones de la capa de distribución la realizan los conmutadores SWL2-PALACIO-R[1-3]-1. Los conmutadores SWL2-PALACIO-R[1-3]-[2-3] realizan las funciones de capa de acceso para la sede Palacio.

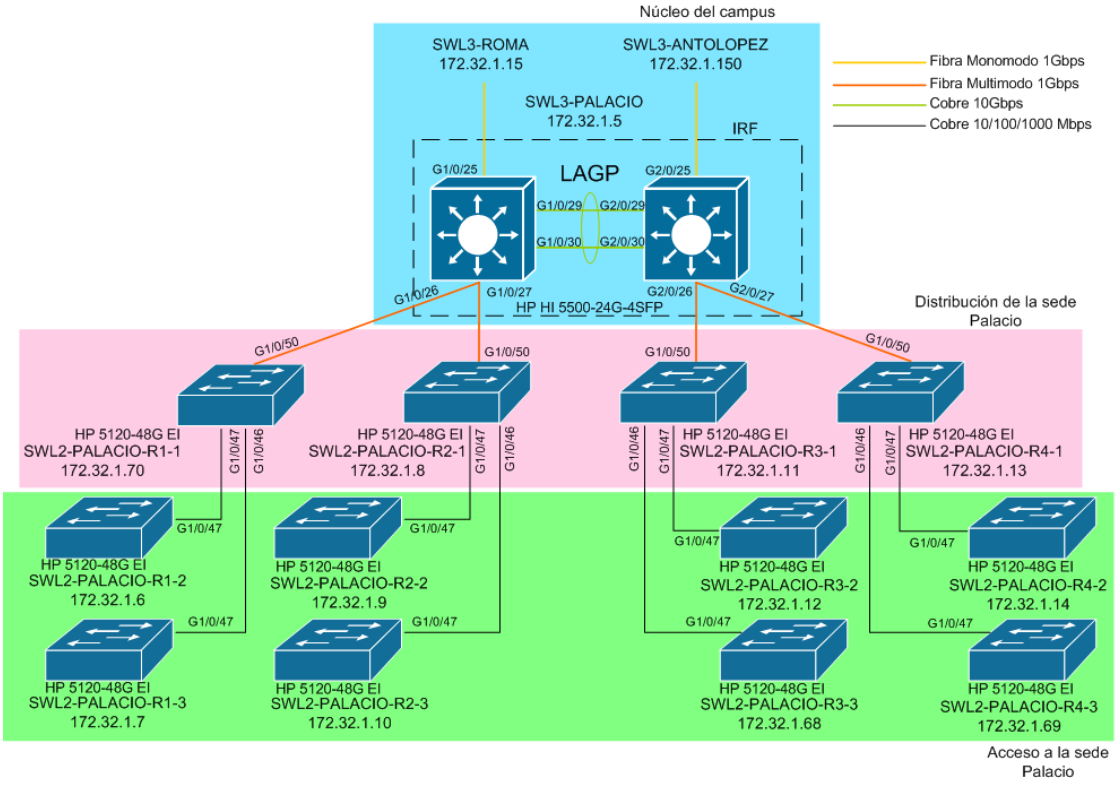


Figura 28 Topología de red de la sede Palacio

3.3.4.10 Sede Roma

La sede Roma posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-ROMA). La topología de red de la sede sigue una arquitectura de dos capas: Núcleo colapsado y acceso. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500. Los conmutadores SWL2-ROMA-[1-5] realizan las funciones de capa de acceso para la sede Roma.

El esquema de la topología de red es el siguiente:

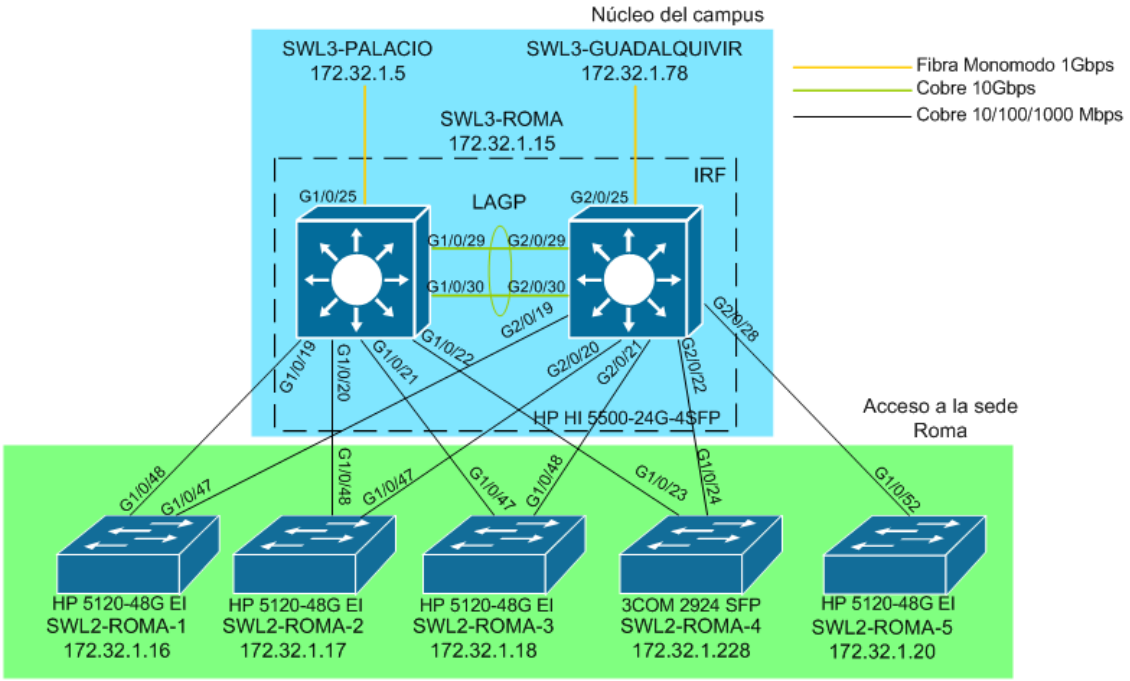


Figura 29 Topología de red de la sede Roma

3.3.4.11 Sede Guadalquivir

La sede Guadalquivir posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-GUADALQUIVIR). Debido al escaso número de equipos de clientes finales activos en la sede, la conexión de los usuarios se proporciona con enlaces directos al clúster. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500, siendo el mismo clúster el que realiza las funciones de capa de acceso para la sede Guadalquivir.

El esquema de la topología de red es el siguiente:

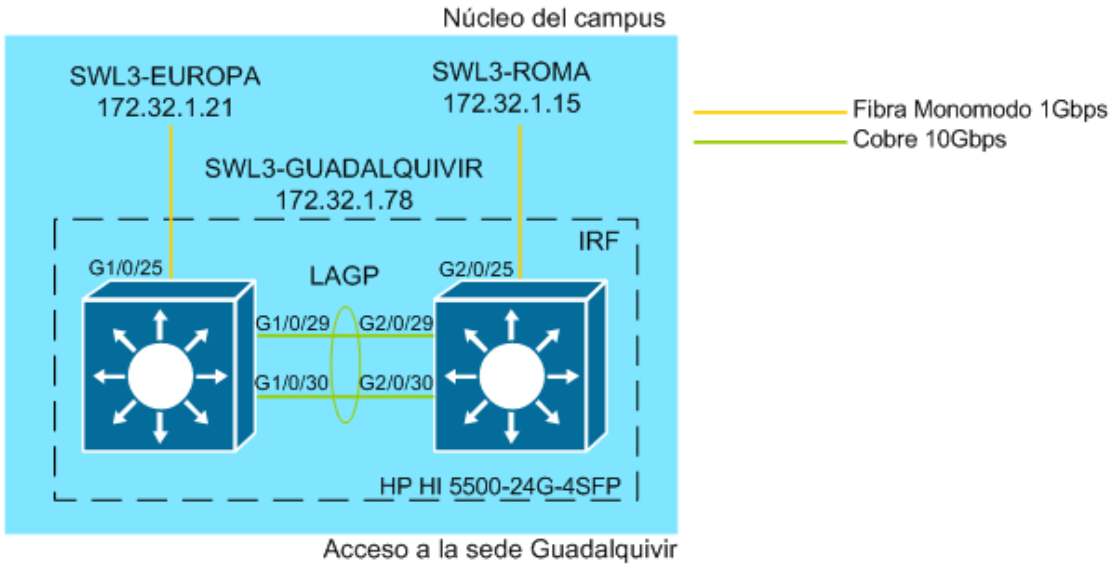


Figura 30 Topología de red de la sede Guadalquivir

3.3.4.12 Sedes Glorieta y Patronado Vivienda

La sede Glorieta posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SWL3-GLORIETA). Debido al escaso número de equipos de clientes finales activos en la sede Glorieta, la conexión de los usuarios se proporciona con enlaces directos al clúster. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500, siendo el mismo clúster el que realiza las funciones de capa de acceso para la sede Glorieta. Las funciones de la capa de acceso para la sede Patronato Vivienda las realiza el conmutador SWL2-PATRONATO_VIVIENDA

El esquema de la topología de red es el siguiente:

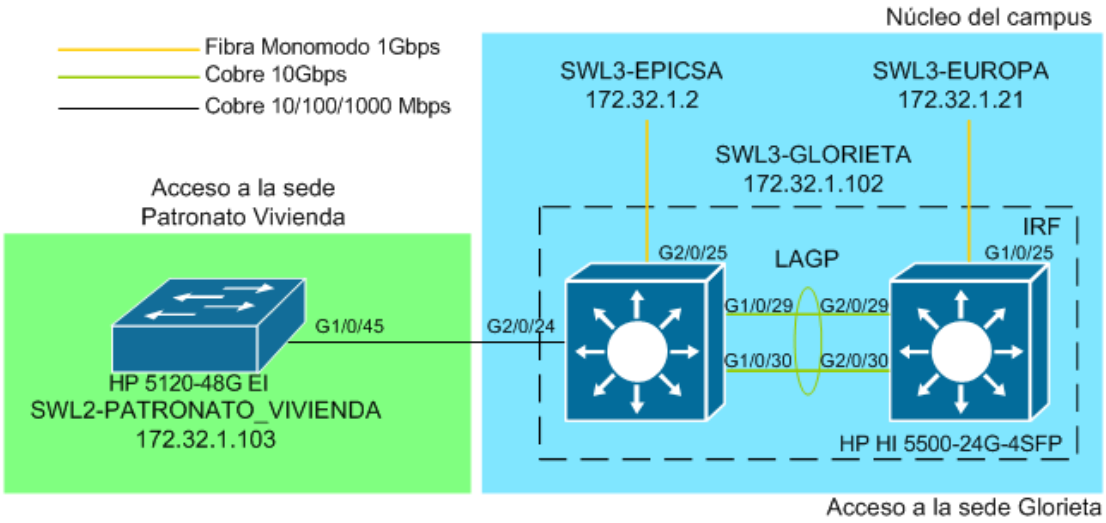


Figura 31 Topología de red de las sedes Glorieta y Patronato Vivienda

3.3.4.13 Sedes Europa y Escuela Hostelería

La sede Roma posee un clúster IRF de dos conmutadores HP 5500 de capa 3 para su conexión al anillo (SLW3-EUROPA). La topología de red de la sede sigue una arquitectura de dos capas: Núcleo colapsado y acceso. La capa de núcleo incluye al clúster IRF de conmutadores HP 5500. Los conmutadores SWL2-EUROPA-RACK[1-10] realizan las funciones de capa de acceso para la sede Roma. El conmutador SWL2-EUROPA_ESCUELA realiza las funciones de capa de acceso para la sede Escuela de Hostelería.

El esquema de la topología de red es el siguiente:

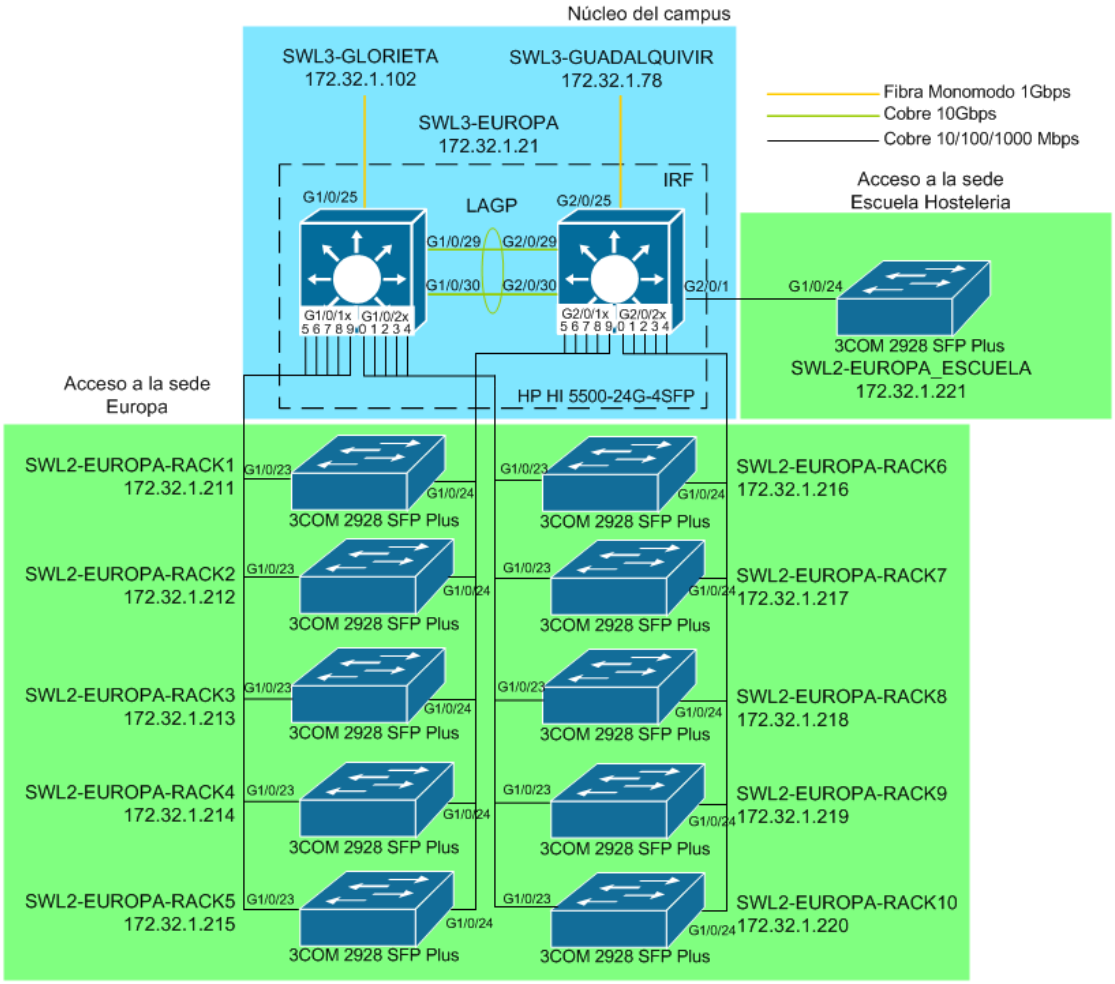


Figura 32 Topología de red de las sedes Europa y Escuela Hostelería

3.3.5 Granja de servidores y centro de datos

Los servidores internos de EPICSA que conforman la granja de servidores y centro de datos, se conectan a la red mediante un clúster IRF de nueve conmutadores HP HI 5500 24G. Dicho clúster de nueve conmutadores se conectan al núcleo del campus empresarial mediante el clúster de 3 conmutadores HP del nodo de EPICSA de la red metropolitana en anillo.

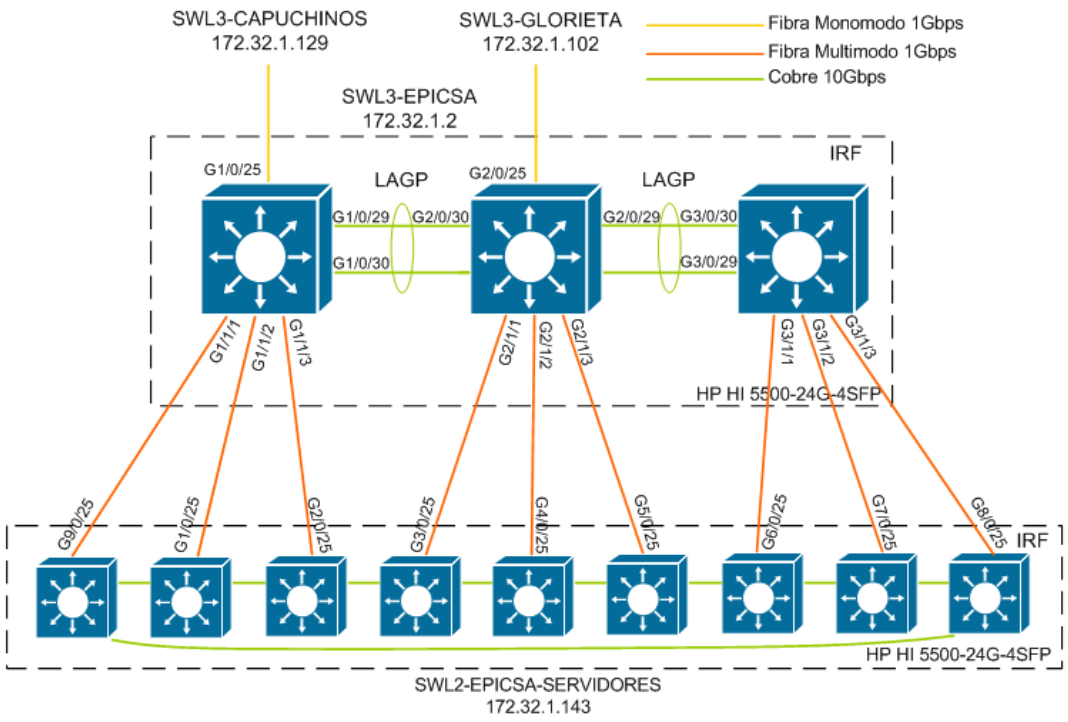


Figura 33 Granja de servidores de EPICSA

Cada uno de los 9 conmutadores que conforman el clúster IRF (SWL2-EPICSA-SERVIDORES) está situado en un rack diferente y presta servicio a todos los servidores situados en dicho rack.

3.4 Borde de la organización

La infraestructura de borde de la organización agrupa la conectividad de varios dispositivos externos al campus de la organización y enruta el tráfico hacia la capa de núcleo de la infraestructura de red interna. Los módulos pertenecientes al área de borde de la organización ofrecen funcionalidades de seguridad que securizan los recursos de la organización cuando se producen conexiones con redes públicas y/o Internet.

La topología lógica del área de borde de la organización, junto con el extremo del ISP y el área remota es la siguiente

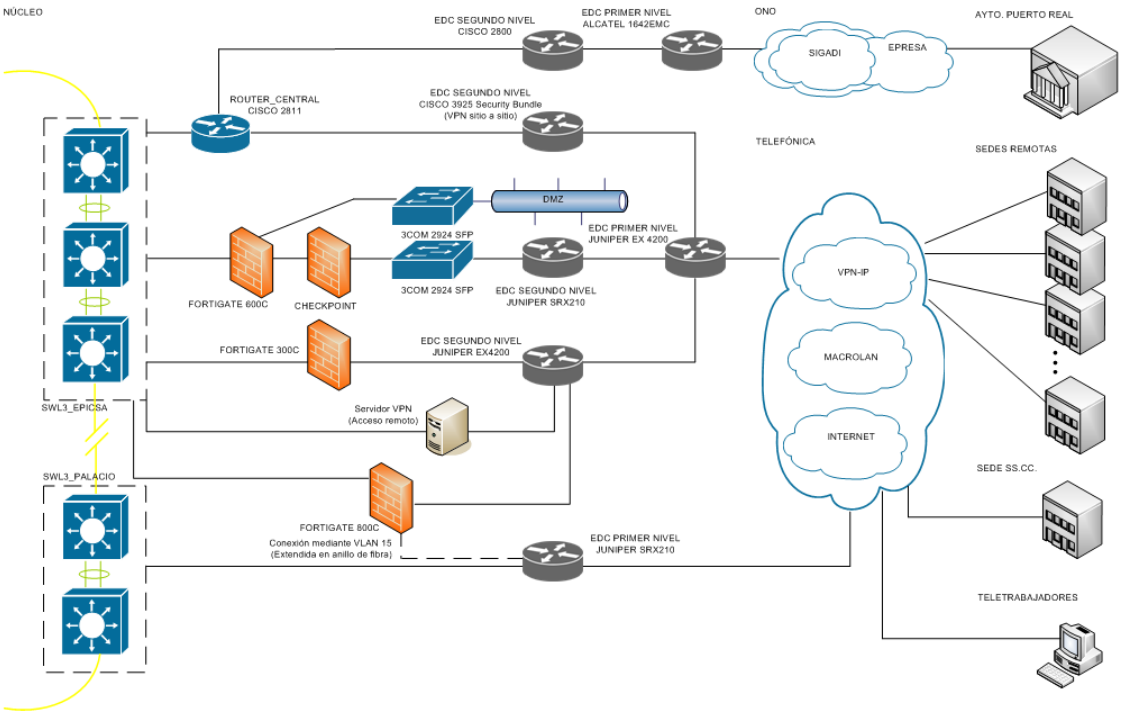


Figura 34 Topología de borde de organización

Para su explicación, se procede a la división de dicha área en módulos tal y como se explica en el libro Wilkins, S. (2011). *Designing for Cisco Internetwork Solutions (DESGN) Foundation Learning Guide:(CCDA DESGN 640-864)*. El resultado es el siguiente:

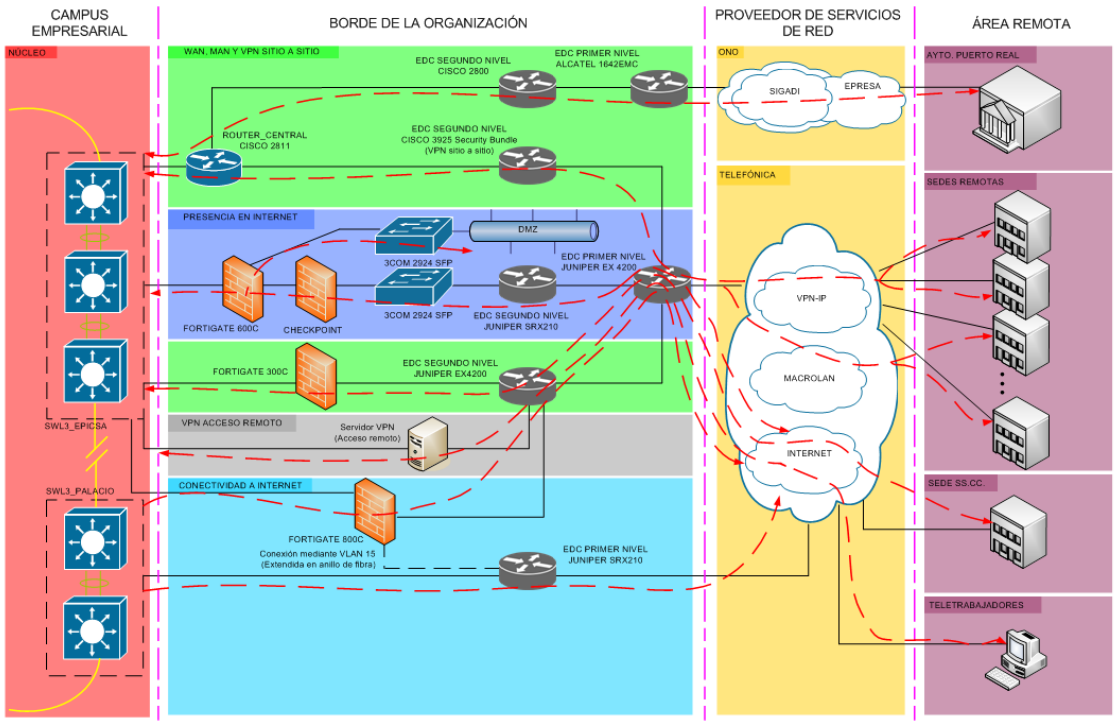


Figura 35 Modularización del borde de la organización

El área de borde de la organización se conecta con el área de campus empresarial a través del nodo clúster IRF de núcleo de conmutadores HP de EPICSA del anillo metropolitano

(SWL3_EPICSA), y, al no existir distribución de borde, la arquitectura resultante es de núcleo colapsado.

3.4.1 Módulo WAN, MAN y VPN sitio a sitio

El módulo de MAN, WAN y VPN sitio a sitio establece conexiones mediante VPN para sedes remotas de la Diputación de Cádiz, ayuntamientos a los que EPICSA presta servicio de datos y aplicaciones y centralitas de VoIP. También se ha desplegado un firewall Fortigate 300C para la gestión de una conexión con la sede de Servicios Sociales y Comunitarios de la Diputación de Cádiz.

3.4.2 Módulo Presencia en Internet

Se ha desplegado una red desmilitarizada (DMZ) para ofrecer servicios corporativos a la red pública. Dicha red DMZ se conecta a la red pública a través de un clúster de firewalls Fortigate 600C, que a su vez se conecta a un clúster de firewalls Checkpoint que se conecta directamente al ISP. El acceso público a la DMZ se realiza a través de estos dos clústeres de firewalls.

3.4.3 Módulo VPN de acceso remoto

Se dispone de un servidor Linux, con firewall propio, desplegado para la gestión de todas las conexiones VPN para tele trabajadores de la Diputación de Cádiz.

3.4.4 Módulo de Conectividad a Internet

El módulo de conectividad a Internet está constituido de la siguiente manera. Para la navegación a Internet de los empleados de la Diputación de Cádiz y de los ayuntamientos a los que EPICSA presta servicio, se ha desplegado un clúster de dos firewalls Fortigate 800C que gestiona las conexiones WAN con el ISP. Se han configurado dos rutas diferenciadas para el acceso a Internet, una en EPICSA y otra en la sede de Palacio. La conexión de Palacio al clúster de firewalls Fortigate 800C, que está físicamente situado en EPICSA, se realiza mediante una extensión lógica a través de la VLAN 15 (Fortigate), extendida en el anillo metropolitano. El clúster de firewalls Fortigate800C se encarga de balancear el tráfico de red del módulo de conectividad a internet entre las dos rutas configuradas en la red de la Diputación de Cádiz: EPICSA y Palacio Provincial.

3.4.5 Caudales de tráfico de red con proveedores

Los caudales de tráfico de red de los que dispone la Diputación de Cádiz son los siguientes:

- **Conexión con Ayuntamiento de Puerto Rea**l, a través del servicio SigADI de ONO.
- **VPNs de Ayuntamientos, sedes remotas y centralitas VoIP**, a través del servicio VPN IP de Telefónica.
- **Presencia Web**, a través del servicio MacroLAN de Telefónica. Este caudal se utiliza para la prestación pública de servicios mediante una DMZ.
- **Conexiones con la sede de Servicios Sociales y Comunitarios de la Diputación de Cádiz**, a través del servicio IP de Telefónica.
- **VPN Teletrabajadores**, a través del servicio IP de telefónica. Este caudal se utiliza para la conexión de teletrabajadores a la red de la Diputación de Cádiz.

- **Navegación**, a través del servicio IP de Telefónica. Este caudal se utiliza para la navegación web de todo el personal interno de la Diputación de Cádiz.

3.5 Proveedor de servicios de red

En la red de la Diputación provincial de Cádiz existen conexiones a diferentes ISP y diferentes servicios de los mismos según el caudal de tráfico correspondiente. Todos los EDC desplegados en la red de la Diputación de Cádiz para conectarse a los diferentes ISP son gestionados por dichos ISP.

3.5.1 ONO

La empresa EPICSA, para ofrecer servicios de datos y aplicaciones al Ayuntamiento de Puerto Real, tiene contratado servicio de red con el proveedor ONO, con las siguientes características:

Concepto	Valor
Servicio	SigADI
Tecnología	HFC
Ancho de banda contratado	10 Mb/s simétricos
EDC Primer nivel	Alcatel 1642EMC
Localización EDC Primer nivel	Sede EPICSA
EDC Segundo nivel	Cisco 2800

Tabla 9 Características del servicio contratado del proveedor ONO

Se tiene contratado con el Proveedor ONO una línea con ancho de banda de 10 Mb/s simétricos. La red del proveedor finaliza en el EDC de segundo nivel que se conecta con el EDC de primer nivel. Es el propio proveedor ONO el que gestiona la línea de conexión con el Ayuntamiento de Puerto Real.

3.5.2 Telefónica

La empresa EPICSA, para ofrecer servicios de datos y aplicaciones a la Diputación de Cádiz (sedes remotas, servicios provinciales de recaudación, ayuntamientos con menos de 20.000 habitantes, etc.), tiene contratado servicio de red con el proveedor Telefónica, con las siguientes características:

Concepto	Valor
Servicio	MacroLAN
Tecnología	VPN IP
Ancho de banda contratado	20 Mb/s simétricos
EDC Primer nivel	Juniper EX4200, Juniper SRX210
Localización EDC Primer nivel	Sede EPICSA y Palacio, respectivamente
EDC Segundo nivel	Juniper EX4200, Juniper SRX210, Cisco 3925 Security Bundle

Tabla 10 Características del servicio contratado del proveedor Telefónica

Se tiene contratado con el Proveedor Telefónica una línea con ancho de banda de 10 Mb/s simétricos. La red del proveedor finaliza en los diferentes EDCs de segundo nivel, desplegados en EPICSA, que se conectan con los dos EDCs de primer nivel. Es el propio proveedor Telefónica el que gestiona las líneas de navegación a Internet, de presencia

corporativa en la web, de VPN sitio a sitio, de conexión con la sede SS.CC de la Diputación de Cádiz y de las VPNs de acceso remoto.

Para la presencia corporativa en la web, se le ha asignado a EPICSA dos bloques de direcciones IP públicas para la prestación de servicios:

- 213.0.62.64/29
- 213.0.60.32/29

La empresa EPICSA no dispone de sistema autónomo propio.

3.6 Área remota

3.6.1 Ayuntamiento de Puerto Real

EPICSA ofrece conexión a la red NEREA de la Junta de Andalucía al Ayuntamiento de Puerto Real a través de los servicios de SigADI de ONO. Se ha desplegado un router Cisco C1700-SV8Y7-M que establece la conexión con la red de la Diputación de Cádiz.

Para la conexión a Internet, el Ayuntamiento de Puerto Real utiliza los servicios de ONO a través de un convenio con la empresa Electricidad de Puerto Real S.A. (EPRESA).

3.6.2 Sedes remotas

La empresa EPICSA ofrece conexión a la red de la Diputación de Cádiz mediante el servicio VPN IP de Telefónica a Servicios Provinciales de Recaudación, sedes remotas de la Diputación de Cádiz y a los ayuntamientos de las ciudades de la Provincia de Cádiz con menos de 20.000 habitantes. La conexión garantiza un ancho de banda mínimo de 2 Mbps. de bajada y 512 Kbps de subida. La lista completa de centros, sedes y ayuntamientos remotos se incluye en el anexo A.

En los ayuntamientos con menos de 20.000 habitantes, la conexión con la red de la Diputación de Cádiz se realiza a través de un router Cisco 887-SEC-K9. Los ayuntamientos disponen de una segunda conexión al exterior para acceder a Internet. Dicha conexión no es responsabilidad de EPICSA, por lo que la elección de ISP, que prestará servicios de conexión a Internet, es competencia del ayuntamiento correspondiente.

Para la conexión a la red de la Diputación de Cádiz de las oficinas de recaudación, también se ha desplegado un router Cisco 887-SEC-K9. El acceso a Internet de las oficinas si es competencia de EPICSA por lo que el servicio lo presta Telefónica a través del convenio existente con la Diputación de Cádiz. La elección y gestión del equipo desplegado en la oficina de recaudación correspondiente para el acceso a Internet son competencias de Telefónica.

El plan de direccionamiento para todos los ayuntamientos y sedes de la Diputación provincial de Cádiz remotas, es el siguiente:

Sede	Grupo	Rack	VLAN	Red	Puerta de enlace
Ayuntamientos	Clientes	Todos	n/a	192.168.[1-51].0/24	192.168.[1-51].1
Oficinas recaudación	Clientes	Todos	n/a	172.22.[32-149].0/24	172.22.[32-149].6

Tabla 11 Plan de direccionamiento de la Red Privada Virtual

3.6.3 Sede Servicios Sociales y Comunitarios

Para la conexión a la red de la Diputación de Cádiz de la sede de Servicios Sociales y Comunitarios, se ha desplegado un router Cisco 887-SEC-K9. El acceso a Internet de la sede si es competencia de EPICSA por lo que el servicio lo presta Telefónica a través del convenio existente con la Diputación de Cádiz. La elección y gestión del equipo desplegado para el acceso a Internet son competencias de Telefónica.

3.6.4 Teletrabajadores

Para la conexión a la red de la Diputación de Cádiz, un teletrabajador puede utilizar cualquier conexión a Internet. Simplemente tiene que conectarse al servidor VPN de EPICSA a través de una dirección IP pública y utilizar el certificado expedido por la misma EPICSA.

4 Normas y referencias

4.1 Disposiciones legales y normas aplicadas

- Norma UNE 157801:2007. Criterios generales para la elaboración de proyectos de sistemas de información.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín Oficial del Estado, núm. 25, de 29 de enero de 2010, páginas 8089 a 8138.

4.2 Bibliografía

- Beale, J., Deraison, R., Meer, H., Temmingh, R., & Walt, C. V. D. (2004). *Nessus network auditing*. Syngress Publishing.
- Bejtlich, R. (2004). *The Tao of network security monitoring: beyond intrusion detection*. Pearson Education.
- Brotherston, L., & Berlin, A. (2017). *Defensive Security Handbook, 1st Edition*. O'Reilly Media, Inc.
- Caswell, B., & Beale, J. (2004). *Snort 2.1 intrusion detection*. Syngress Publishing.
- Mañas, J.A (2013). *Guía de implantación del ENS, Guía de seguridad CCN-STIC 804*.
- Rowland, C. H. (2002). *U.S. Patent No. 6,405,318*. Washington, DC: U.S. Patent and Trademark Office.
- Sun, M., & Chen, T. (2010). *U.S. Patent Application No. 12/411,916*.
- USM Appliance™ User Guide. (2017). [ebook] AlienVault. Disponible en: https://www.alienvault.com/documentation/resources/pdf/usm-appliance-user-guide.pdf [Accedido 3 Mar. 2017].
- USM Appliance™ Deployment Guide. (2017). [ebook] AlienVault. Disponible en: https://www.alienvault.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf [Accedido 3 Mar. 2017].
- Wilkins, S. (2011). *Designing for Cisco Internetwork Solutions (DESGN) Foundation Learning Guide:(CCDA DESGN 640-864)*. Pearson Education.

4.3 Métodos, herramientas, modelos, métricas y prototipos

- **Microsoft Word 2013**. Editor de texto utilizado para la elaboración del documento final.
- **Microsoft Visio 2003**. Editor de gráficos utilizado para la visualización y edición de los planos de red.
- **GanttProject**. Editor de diagramas de Gantt utilizado para la realización del diagrama de planificación del proyecto.

5 Definiciones y abreviaturas

- **ARP**: Protocolo de resolución de direcciones.
- **CVE**: Common Vulnerabilities and Exposures.
- **DIDS**: Sistema distribuido de detección de intrusos.
- **DNS**: Sistema de nombres de dominio.
- **EDC**: Equipo en domicilio del cliente.
- **FTP**: Protocolo de transferencia de ficheros.
- **HIDS**: Sistema de detección de intrusos en host.
- **HTTP**: Protocolo de transferencia de hipertexto.
- **ICMP**: Protocolo de mensajes de control de internet
- **IDS**: Sistema de detección de intrusos.
- **IMAP**: Protocolo de acceso a mensajes de internet.
- **IP:** Protocolo de internet.
- **IPS**: Sistema de prevención de intrusiones.
- **Kbps**: Kilobits por segundo.
- **MAC**: Control de acceso al medio.
- **MBps**: Megabytes por segundo.
- **Mbps**: Megabits por segundo.
- **NIDS**: Sistema de detección de intrusos en red.
- **OSSIM**: Administración de la seguridad de la información de código abierto.
- **POP3:** Protocolo de oficina de correo.
- **RADIUS**: Protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.
- **SIEM**: Administración de seguridad de la información y eventos.
- **SMTP**: protocolo para transferencia simple de correo
- **SNMP**: Protocolo simple de administración de red.
- **SPAN**: Analizador de puerto conmutado.
- **SSL**: Capa de puertos seguros.
- **TAP**: Dispositivo de red que permite separar la entrada de datos de la salida de datos.
- **TCP**: Protocolo de control de transporte.
- **UDP**: Protocolo de datagrama de usuario.
- **VPN**: Red virtual privada.

6 Requisitos iniciales

Basándonos en la entrevista realizada a Manuel Añón Rodríguez, coordinador del departamento de redes y telecomunicaciones de la Empresa Provincial de Información de Cádiz S.A. (EPICSA), se establecen los siguientes requisitos iniciales del sistema de información de seguridad y administración de eventos:

- **R-01**: Debe proporcionar información sobre alertas de seguridad producidas en la zona frontera de la red interna de la Diputación de Cádiz.
- **R-02**: Debe proporcionar información sobre las vulnerabilidades de los activos de la red.
- **R-03**: Debe proporcionar información sobre alertas de seguridad producidas en los equipos con sistema operativo Windows de la Diputación de Cádiz.
- **R-04**: Debe proporcionar información administrativa de la red de datos (listado de activos, estadísticas de uso, etc.).
- **R-05**: Debe definir niveles de importancia para los activos de la empresa.
- **R-06**: Debe permitir el acceso simultáneo de diferentes usuarios administradores.
- **R-07**: Debe permitir el almacenamiento prolongado de los registros.
- **R-08**: Debe tener un sistema de copias de seguridad de los registros.

7 Alcance

Este proyecto se aplica a la definición e implantación de un sistema de información de seguridad y administración de eventos en la red interna de la Diputación Provincial de Cádiz.

Este proyecto incluye:

- Estudio de la red interna de la Diputación Provincial de Cádiz.
- Especificación de requisitos del sistema de información de seguridad y administración de eventos en base a una entrevista con EPICSA.
- Análisis de las alternativas en el despliegue del SIEM.
- Descripción de las soluciones propuestas.
- Estudio teórico sobre el diseño modular de una red.
- Estudio teórico sobre la monitorización de redes.
- Estudio teórico sobre la detección de intrusiones.
- Estudio teórico sobre el análisis de vulnerabilidades.
- Estudio teórico sobre sistemas de información de seguridad y administración de eventos (SIEM).
- Guía de instalación y actualización del SIEM.
- Establecimiento de mediciones de recursos para la consecución del proyecto.
- Elaboración de un presupuesto para la consecución del proyecto.

8 Estudio de alternativas y viabilidad

En este apartado se estudiarán las posibles alternativas a considerar en la consecución de este proyecto. Las siguientes alternativas se desarrollarán en los apartados sucesivos.

Concepto	Alternativas a estudiar
Software	OSSIM, USM, SIEM Privativo
Hardware	CPU, RAM, HDD, Interfaces de red
Localización de los sensores	Frontera, DMZ, LAN
Despliegue	Red en línea, red fuera de línea
Configuración del SIEM	Detección de intrusiones, Análisis de vulnerabilidades

Tabla 12 Resumen de estudio de alternativas y viabilidad

8.1 Software

La elección del sistema de información de seguridad y administración de eventos que se vaya a implantar en una red dependerá de varios factores, principalmente, del número de activos a monitorizar y del presupuesto disponible por parte de la organización para la adquisición del mismo.

Para empresas con pocos activos que monitorizar, la adquisición de una licencia de un SIEM privativo puede ser algo asequible. Pero, para una empresa con muchísimos activos que monitorizar, la adquisición de una licencia puede ser bastante más costosa.

La existencia de un SIEM de código abierto como OSSIM, ofrece la posibilidad de la adquisición de un SIEM de manera gratuita, limitado únicamente por el hardware sobre el que se despliega. Sin ningún tipo de restricción en cuanto al número de activos a monitorizar, OSSIM ofrece una solución atractiva para empresas con muchísimos activos que no deseen invertir demasiados recursos económicos en licencias privativas. Además, la continúa actualización de las bases de datos de vulnerabilidades, de las firmas de ataques en red y de la continúo mantenimiento gratuito por parte de la empresa desarrolladora de OSSIM, hacen de este SIEM una solución muy económica y adaptable para todas las organizaciones.

La empresa desarrolladora del SIEM OSSIM ofrece también dos versiones con licencia de pago, denominadas USM Appliance y USM Anywhere. La diferencia principal con OSSIM, es que ambas versiones de USM reciben actualizaciones diarias sobre patrones de ataques más complejos que los ofrecidos por las firmas de los IDS. En OSSIM se pueden establecer dichos patrones complejos, pero no se actualizan por parte de la empresa. Las versiones de pago ofrecen un almacenamiento basado en bases de datos NoSQL de más larga duración que el de OSSIM. La empresa también ofrece el suministro de hardware especializado en la ejecución del SIEM USM que se adquiera, para conseguir un rendimiento óptimo.

8.2 Hardware

En un despliegue de un sistema de información de seguridad y administración de eventos, hay que tener en cuenta que tenemos dos tipos de perfiles de máquinas: servidor de recolección y análisis de eventos y sensores de monitorización del tráfico de red.

Dependiendo del propósito que tenga la máquina dentro de nuestro SIEM, los requerimientos hardware varían.

8.2.1 Hardware del servidor

Dentro de un sistema SIEM, el servidor se encarga de recolectar todos los eventos de seguridad generados en los diferentes sensores desplegados por la red monitorizada y/o agentes instalados en los diferentes activos de la empresa. Un servidor SIEM debe tener una capacidad de almacenamiento amplia para proveer almacenamiento de larga duración de todos los eventos de seguridad e información de activos y de la red de la empresa, sobre todo para el cumplimiento de las normativas aplicables a los procedimientos de la organización correspondiente.

Es difícil de determinar con exactitud cuál es la capacidad de almacenamiento exacta para un determinado despliegue de un servidor SIEM, pues dependerá de diversos factores, como:

- Número de activos a monitorizar.
- Número de sensores desplegados.
- Ancho de banda de la red.
- Porcentaje de falsos positivos generados.

También hay que tener en cuenta que los factores anteriores determinan la capacidad de procesamiento del servidor, puesto que, mientras más aumentan esos factores, mas capacidad de cómputo (CPU y RAM) debe poseer el servidor para realizar todo el análisis posterior de la información de seguridad.

Es muy difícil definir unos requisitos hardware mínimos a la hora de desplegar un servidor SIEM debido a la heterogeneidad existente en las redes estructuradas actuales, pero las recomendaciones generales son:

- CPU de 64 bits, más de 2 núcleos y, como mínimo, 2,4 GHz de frecuencia.
- Memoria RAM entre 16 y 24 GB.
- Almacenamiento masivo mayor de 125 GB.

En cuanto a las interfaces de red necesarias y su ancho de banda, lo usual es que un servidor SIEM tenga dos interfaces de red instaladas, una para administración y otra para recolección de eventos, aunque puede darse el caso de que se utilice sólo una interfaz de red para ambos propósitos. La velocidad de la/s interfaz/ces de red dependerá de los eventos de seguridad por segundo que recibirá el servidor. Lo normal es que el ancho de banda de las interfaces de red de un servidor SIEM varíen entre los 100 Mbps y los 1000 Mbps.

8.2.2 Hardware del sensor

Dentro de un sistema SIEM, el sensor se encarga de analizar todo el tráfico de red y generar alertas de seguridad para el servidor SIEM según diversos factores. La característica principal y más importante a la hora de analizar los requisitos hardware de un sensor SIEM es el ancho de banda de sus interfaces de red. Un sensor SIEM debe poseer un ancho de

banda en las interfaces de red de monitorización que le permitan soportar todo el tráfico que transita la red monitorizada.

Normalmente, la interfaz de red para monitorizar en el sensor SIEM deberá tener un ancho de banda, como mínimo, igual a la red monitorizada o, en algunos casos, al ancho de banda del enlace específico que se vaya a monitorizar. Por ejemplo, si la red a monitorizar tiene un ancho de banda de 1000 Mbps, la interfaz de red el sensor SIEM que vaya a monitorizar el tráfico de red deberá ser de, como mínimo, 1000 Mbps.

También hay que tener en cuenta que un sensor SIEM debe poseer un bus en sus puertos PCI que le permita soportar toda la captura de paquetes que se realiza en sus interfaces de monitorización, ya sean varias o una sola. Por ejemplo, veamos dos anchos de banda de dos puertos PCI diferentes

- PCI 32 bits a 33 MHz ofrece un ancho de banda de 133 MBps o 1,064 Mbps.
- PCI-Express 64 bits a 66 MHz ofrece un ancho de banda de 533 MBps o 4,264 Mbps.

En el siguiente cuadro podemos ver la posible saturación que puede producirse en el sensor según las interfaces de red que tenga dicho sensor, el ancho de banda de dichas interfaces y el puerto PCI del sensor.

NICs	Ancho de banda NICs (Mbps)	Saturación PCI 32b	Saturación PCI-Express
1	10/100	No	No
2	10/100	Sí	No
1	1000	Sí	No
2	1000	Sí	No

Tabla 13 Saturación de PCI según las NICs de un sensor SIEM

Se puede ver que para un sensor SIEM con una interfaz de red con ancho de banda de 10/100 Mbps, basta con un PCI de 32 bits a 33 MHz pero, a partir de ahí, se recomienda un puerto PCI Express de 64 bits de, como mínimo, 66 MHz de ancho de banda.

En un despliegue habitual de un sistema SIEM, los sensores tienen, como mínimo, dos interfaces: una para administración y todas las demás para monitorizar el tráfico de red.

Para un sensor SIEM, la capacidad de almacenamiento masivo y de memoria RAM son menos importantes, pero debe ser, como mínimo, aquella que permita un correcto funcionamiento del sensor SIEM.

8.3 Localización de los sensores

El objetivo de los sensores en un sistema SIEM es el de analizar todo el tráfico de red que circula por ellos e identificar qué trafico es factible de ser considerado un intento de ataque, o cualquier otro tipo de comportamiento sospechoso.

Para que la tarea de los sensores de un sistema SIEM sea lo más eficaz posible, hay que tener en cuenta dónde se van a colocar dichos sensores en la red a monitorizar, puesto que hay que intentar llegar a un estado donde los sensores SIEM sean capaces de analizar el máximo tráfico de red posible. La aproximación habitual en un despliegue de sensores

SIEM en una red de datos es colocarlos en los puntos frontera entre las diferentes áreas definidas en una red, ya sean áreas conocidas como una DMZ, la salida a Internet o la Intranet, o áreas definidas por cada organización como áreas de departamentos.

A la hora de desplegar un sistema SIEM con sus sensores específicos, hay que tener en cuenta que, según dónde se coloquen dichos sensores, habrá tráfico de red que puedan analizar, y otro tráfico de red que no puedan analizar por el simple hecho de que no atraviesa la zona de la red dónde están desplegados los sensores. Por ejemplo, si tenemos en cuenta la siguiente topología de red típica de una organización, vemos que tenemos tres zonas a monitorizar: LAN, salida a Internet y DMZ.

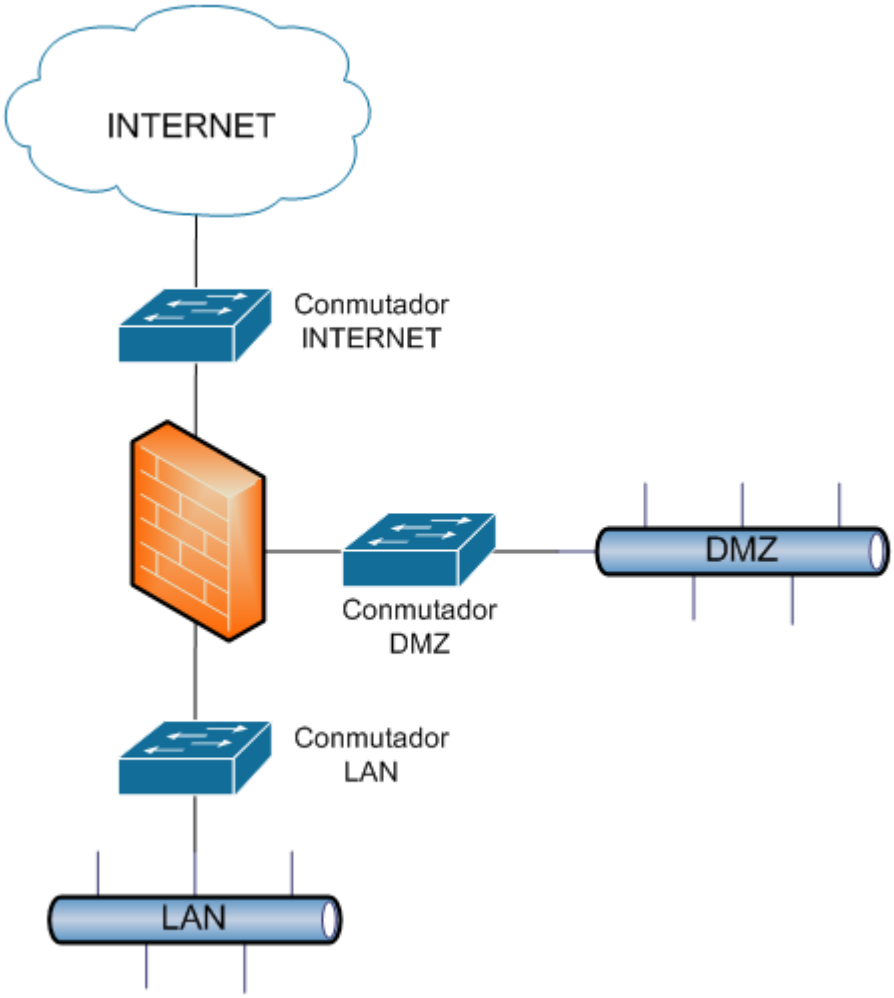


Figura 36 Zonas de una red conmutada para localización de sensores SIEM

Para analizar el tráfico de cada zona debemos colocar un sensor en un puerto espejo del conmutador que conecte dicha zona con el cortafuegos central. Dependiendo de donde coloquemos el sensor, habrá tráfico que pasará por él, y tráfico que no. Veamos las tres posibilidades:

1. **Conmutador LAN**. Si colocamos el sensor en un puerto espejo del conmutador que conecta la LAN con el cortafuegos central, el sensor será capaz de analizar todo el tráfico que transita la DMZ y la LAN y la LAN e Internet, siendo ambos

tránsitos bidireccionales. Un sensor en esta localización no sería capaz de analizar el tráfico de red que transita Internet y la DMZ.

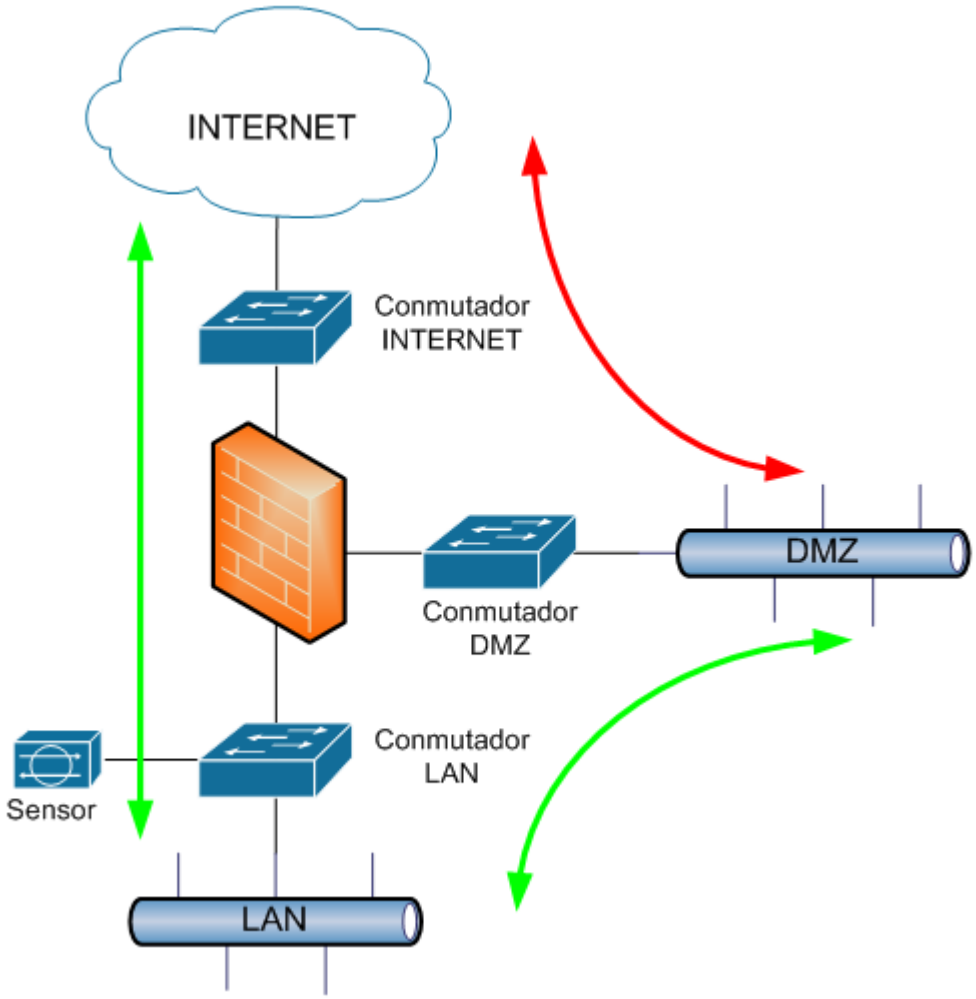


Figura 37 Sensor SIEM en salida de LAN

2. **Conmutador DMZ**. Si colocamos el sensor en un puerto espejo del conmutador que conecta la DMZ con el cortafuegos central, el sensor será capaz de analizar todo el tráfico que transita la DMZ y la LAN y la DMZ e Internet, siendo ambos tránsitos bidireccionales. Un sensor en esta localización no sería capaz de analizar el tráfico de red que transita Internet y la LAN.

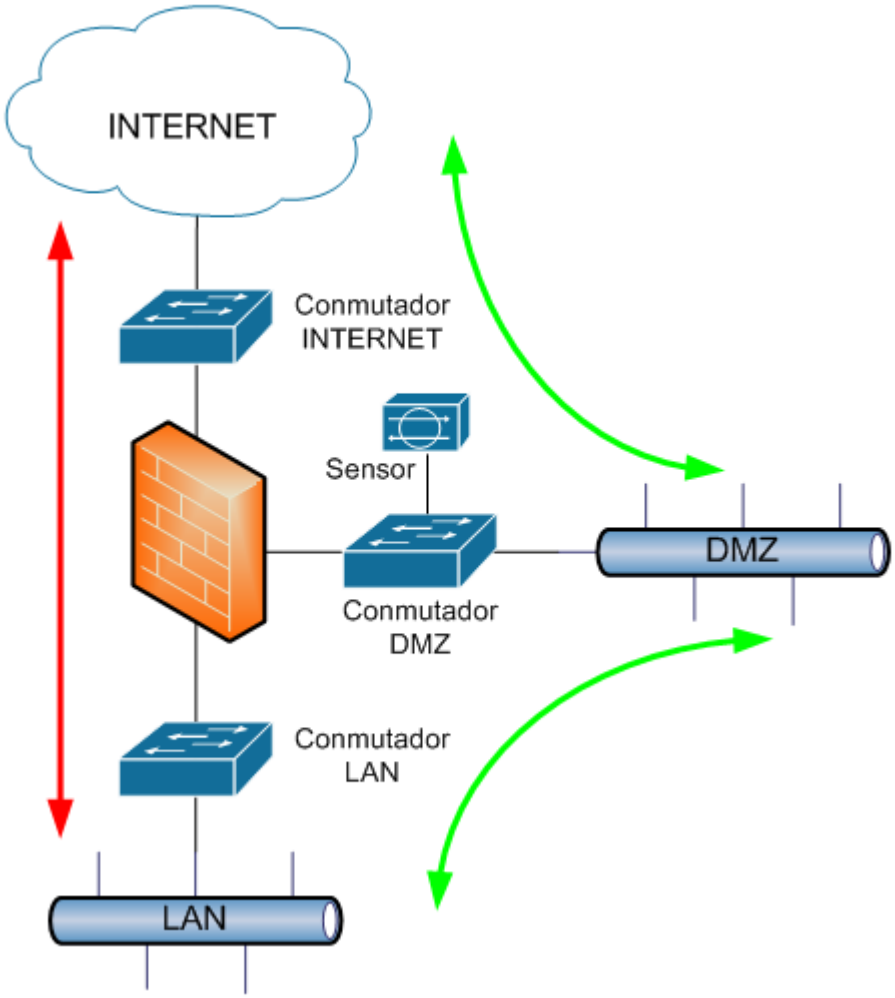


Figura 38 Sensor SIEM en salida de DMZ

3. **Conmutador Internet**. Si colocamos el sensor en un puerto espejo del conmutador que conecta Internet con el cortafuegos central, el sensor será capaz de analizar todo el tráfico que transita Internet y la LAN y la DMZ e Internet, siendo ambos tránsitos bidireccionales. Un sensor en esta localización no sería capaz de analizar el tráfico de red que transita la DMZ y la LAN.

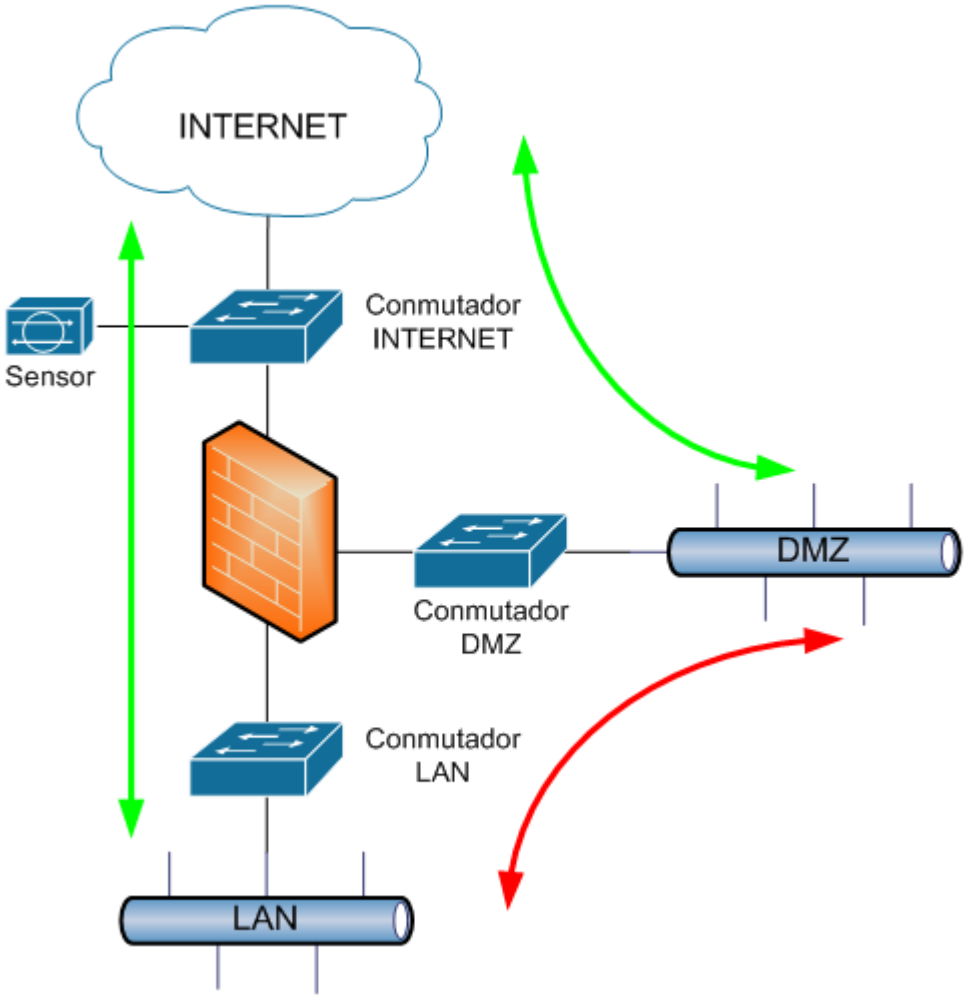


Figura 39 Sensor SIEM en salida a Internet

Qué localización para un sensor SIEM es más importante para una organización dependerá de la configuración específica, las áreas que se consideren más valiosas y las áreas que se consideren más factibles de sufrir un ataque, tanto externo como interno. En un caso ideal, los sensores sería desplegados en todos los puntos posibles de una red de datos para no dejar sin monitorizar ningún área de dicha red, pero, por motivos de coste, esto es, en muchos casos, imposible. Por lo tanto, se debe analizar qué áreas son más importantes para la organización y estudiar las posibles localizaciones para conseguir una monitorización óptima de todo el tráfico que transita dichas áreas.

8.4 Despliegue

A la hora de desplegar una red de sensores SIEM en una red corporativa, hay que tener en consideración que se necesita de una red de monitorización que interconecte los sensores con un punto central de administración, para la gestión y administración de dichos sensores y para el envío de las alertas de seguridad generadas en los sensores.

Para desplegar una red de sensores SIEM, tenemos dos alternativas principales:

- Red de monitorización fuera de línea
- Red de monitorización en línea.

8.4.1 Red de monitorización fuera de línea

Esta técnica de despliegue de una red de monitorización consiste en separar físicamente la red de gestión y envío de alertas de la red a monitorizar, con el fin de que dichas redes no compartan ningún tipo de medio físico.

Podemos ver en la figura siguiente un ejemplo de red de monitorización fuera de línea:

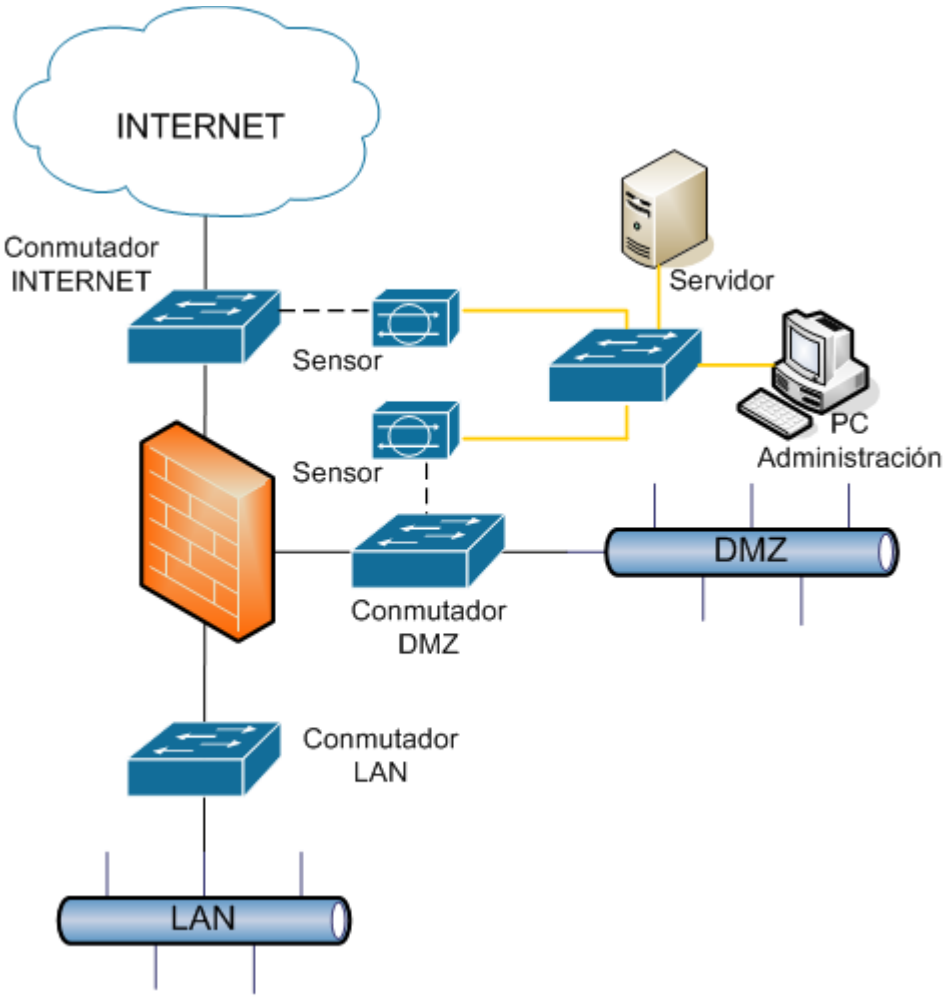


Figura 40 Red de monitorización fuera de línea

En este caso, se puede ver como ambos sensores están conectados a la red a monitorizar para recolectar todo el tráfico de red y analizarlo. La red de envío de alertas al servidor y de administración centralizada está separada físicamente de la red a monitorizar para evitar que un posible atacante externo detecte los registros de alertas y detecte que está siendo monitorizado. Otra ventaja de esta técnica es que no introduce ningún tipo de latencia en la red a monitorizar, puesto que todo el tráfico de gestión y alerta que se genera en la red de monitorización no transita la red a monitorizar. Para la red a monitorizar, el despliegue de una red de monitorización fuera de línea sería totalmente transparente. La desventaja del uso de esta técnica es que conlleva el diseño de una nueva red estructurada que, en algunos casos, puede ser trivial pero, en otros casos, puede ser más difícil. El diseño de la nueva red también conlleva todos los gastos de personal en el diseño de dicha red y de hardware de red para el despliegue.

8.4.2 Red de monitorización en línea

Esta técnica de despliegue de una red de monitorización consiste en el uso de la red corporativa ya existente para el envío de alertas de seguridad y la administración centralizada de todo el sistema SIEM.

Podemos ver en la figura siguiente un ejemplo de red de monitorización en línea:

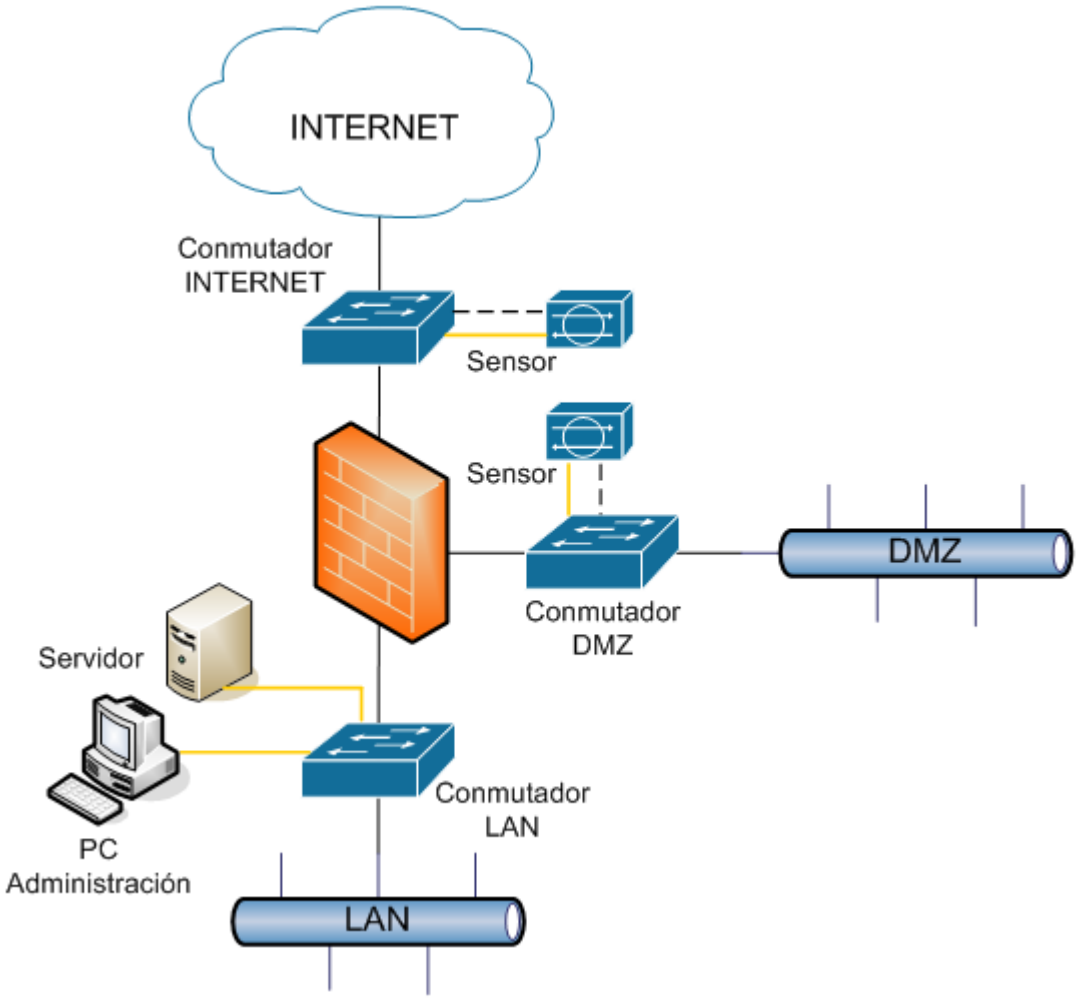


Figura 41 Red de monitorización en línea

En este caso, se puede ver como los sensores están conectados por duplicado a los conmutadores, de tal manera que un enlace sirve para monitorizar la red y otro enlace sirve para el transporte del tráfico de alertas y administración del sensor. Tanto el servidor de almacenamiento como el PC de administración están conectados a la red interna de manera directa para acceder a todo el tráfico de la red de monitorización.

Al estar el tráfico de la red de monitorización transitando la red a monitorizar, se dan dos desventajas:

- Un atacante que se ha introducido en la red corporativa podría detectar el tráfico de la red de monitorización y detectar que está siendo monitorizado.

- El tráfico de red de alertas y administración generado por la red de monitorización podría introducir latencias en la red corporativa si esta no tiene el suficiente ancho de banda o su carga habitual no soporta todo el tráfico de red nuevo.

Una posible solución a la desventaja de la detección por parte de un atacante de la red de monitorización es encriptar todo el tráfico de dicha red de monitorización a través de túneles SSL, SSH o IPSec. Si se lleva a cabo esta técnica, se recomienda configurar ACLs en el firewall correspondiente para controlar los accesos a los sensores.

La ventaja principal de esta técnica reside en el poco coste de despliegue que conlleva, en lo referente al diseño de una nueva red estructurada de datos, puesto que la red sobre la que va a transitar todo el tráfico de la red de monitorización ya está desplegada.

8.5 Configuración del SIEM

8.5.1 Detección de intrusiones

El análisis principal que hay que realizar a la hora de configurar la detección de intrusiones de un sistema SIEM es si se va a implantar una estrategia de bueno conocido o de malo conocido.

Una estrategia de bueno conocido implica un análisis de tráfico continuo para el establecimiento de un comportamiento estándar de una red. Esto puede ser factible en una red más o menos pequeña, pero en una red más grande y heterogénea, la implantación de esta estrategia supone tener muy claro el tráfico que se permite en la red y por tanto tener una política de seguridad muy restrictiva. La ventaja de esta estrategia es que delimita de manera bastante certera la identificación de ataques, al eliminar en gran medida los falsos positivos y, además, permite identificar usos indebidos de la red, aunque ello no suponga un ataque informático.

La otra estrategia que se puede implantar es la de malo conocido, que se basa en el análisis del tráfico de red mediante patrones de ataques conocidos para establecer que tráfico de red es factible de ser malicioso y cual no. Esta estrategia no requiere de un establecimiento de patrones de comportamiento de la red, por lo que no supondría grandes recursos de cómputo. Esta estrategia se adapta a cualquier tipo de red. La desventaja de esta estrategia es que, en la actualidad, las tipologías de ataques y sus procedimientos varían constantemente, y, si no se mantienen totalmente actualizados los patrones de ataques a buscar en la red monitorizada, podemos dejar pasar inadvertido mucho tráfico malicioso en la red.

También existen alternativas a la hora de establecer si un IDS es capaz de ofrecer respuestas activas o pasivas. La elección de un tipo de respuesta u otro dependerá de la proporción de falsos positivos que el IDS genere. Si un IDS genera muchos falsos positivos, la respuesta activa no es una opción, puesto que se cortarían muchas conexiones legítimas. En ese caso, el IDS debería ser pasivo y, posteriormente, el analista debe establecer que tráfico pertenece a un ataque y cual no. Si la proporción de falsos positivos es baja, un IDS con respuesta activa es una buena opción.

8.5.2 Análisis de vulnerabilidades

Cuando se va a configurar un análisis de vulnerabilidades en un sistema SIEM, tenemos varias alternativas.

Si analizamos las alternativas desde el punto de vista de dónde lanzar el análisis, tenemos dos opciones:

- Análisis en equipos.
- Análisis en red.

En una red pequeña con pocos activos, el análisis en equipos es algo factible, ya que no es difícil gestionar cada uno de los análisis por separado. En una red corporativa con muchos activos, gestionar los análisis en particular para cada uno puede ser muy complicado. En ese caso, el análisis en red, que provee de la posibilidad de lanzar el análisis a todos los equipos que se conecten a una red de manera centralizada, es mejor opción.

Otra decisión que se debe tomar a la hora de configurar un análisis de vulnerabilidades es la posibilidad de que ese análisis se realice con las credenciales de los equipos, lo que sería la perspectiva del administrador, o, en el caso contrario, se realice con la perspectiva de un atacante externo. En una red homogénea donde todos los activos utilizan el mismo medio de autenticación, la perspectiva de administrador puede tener sentido, pero en una red donde hay muchos activos diferentes, gestionar las credenciales puede ser complicado, por lo que la perspectiva de un atacante externo puede ser más factible.

9 Descripción de la solución propuesta

9.1 Solución software

La red provincial de la Diputación de Cádiz, la cual gestiona EPICSA, engloba un gran número de activos. Es una red con muchos activos de diferente tipología (equipos personales, servidores, impresoras,…), que generan una gran cantidad de tráfico de diferente tipo (TCP, ICMP, ARP,…).

Si se realiza un cálculo del máximo de activos a monitorizar que la red podría poseer en un momento determinado. La red de la Diputación de Cádiz proporciona conexión a 18 sedes de la Diputación de Cádiz, lo que se traduce en 23 bloques (las sedes EPICSA, Patronato y Roma tienen más de un bloque asignado) de direcciones IP con máscara de subred de 24 bits, es decir, subredes de clase C, que pueden albergar, como máximo, 254 equipos a la vez. La red desmilitarizada, con sede en EPICSA, posee un bloque de direcciones IP clase C. La red de servidores tiene asignada un bloque de direcciones IP con máscara de subred de 19 bits, lo que se traduce en 8.180 activos, como máximo.

*(24 Redes C * 254 Activos/Red C) + (1 Red de máscara 19 * 8180 Activos/Red)* = ***14.276 activos***.

En el peor caso posible, la red de la Diputación de Cádiz estaría soportando el tráfico de red de 14.276 activos, que sería el mismo número de activos a monitorizar por el SIEM. Este es el factor más determinante a la hora de seleccionar un SIEM, ya que, todos los

SIEMs que ofrecen licencias limitadas a un cierto número de activos a monitorizar, no se acercan a la cifra de activos posibles de la red de la Diputación de Cádiz.

El SIEM que se vaya a desplegar en la red de la Diputación de Cádiz debe ser lo suficientemente versátil como para soportar la gran cantidad de activos presentes en la red, así como la variedad de tráfico que se va a monitorizar. Por ello, el software elegido es OSSIM, ya que es de código abierto y no ofrece ningún tipo de limitación en lo referente a licencias ni número de activos a monitorizar y, si el hardware sobre el que OSSIM está instalado posee la suficiente capacidad, la escalabilidad de OSSIM es muy considerable.

Figura 42 Logo AlienVault OSSIM

Además, OSSIM ofrece en la misma instalación una gran cantidad de software libre que cumplen con los requisitos establecidos por EPCISA para la realización de este proyecto:

- **Requisito R-01**: Suricata, NIDS para alertas de seguridad en el tráfico de red.
- **Requisito R-02**: OpenVAS, escáner de vulnerabilidades.
- **Requisito R-03**: OSSEC, HIDS para alertas de seguridad en equipos.
- **Requisito R-04**: Nagios, inventario de activos.

Para el cumplimiento del resto de requisitos establecidos por EPICSA para la realización de este proyecto, el sistema OSSIM también ofrece las siguientes funcionalidades:

- **Requisito R-05**: Gestión de niveles de valor de activos.
- **Requisito R-06**: Gestión de usuarios.
- **Requisito R-07**: Almacenamiento de las alertas e información de seguridad.
- **Requisito R-08**: Gestión de copias de seguridad de alertas e información de seguridad y configuración del sistema SIEM.

En apartados sucesivos se expondrán las características específicas de cada funcionalidad de OSSIM, así como se ha configurado cada una para adaptarse a la perfección a las características y necesidades de la red de la Diputación de Cádiz.

OSSIM también ofrece la posibilidad de desplegar todo el sistema SIEM (servidor, base de datos, sensores, framework) en una sola máquina o, por el contrario, separar cada uno de los componentes en diferentes máquinas. En el caso de este proyecto, se ha decidido instalar el servidor SIEM en una máquina, junto con la base de datos y el framework para dejar el perfil de sensor libre para su instalación en todas las máquinas separadas que sean necesarias. Así no tenemos un único punto de fallo en el sistema y conseguimos distribuir

la carga de trabajo en diferentes máquinas para que una máquina no tenga que soportar toda la carga que supone la ejecución de OSSIM.

Una de las características principales de OSSIM, es su conexión con AlienVault Open Threat Exchange. OTX es una comunidad global de seguridad en la que participan más de 50.000 expertos en seguridad de más de 140 países, que contribuyen con más de 10 millones de indicadores de peligro actualmente. OTX permite que toda la comunidad comparta y valide toda la información posible sobre peligros emergentes. OTX se basa en la suscripción a pulsos. Un pulso es un conjunto de información determinada que involucra el compromiso de un sistema relacionado con un peligro emergente, por ejemplo, direcciones IP, hashes MD5 de ficheros, dominios. Cuando aparece en la red información relacionada con un pulso, el sistema OSSIM alerta de que hay un problema de seguridad relacionado con dicho pulso.

9.2 Solución hardware

9.2.1 Hardware del servidor

Debido a los altos requerimientos de hardware y a las características de la red de la Diputación de Cádiz (Alto número de activos, red de, como máximo 1 Gbps,…) la máquina sobre la que se vaya a instalar el servidor SIEM debe cumplir, como mínimo, los requisitos dispuestos en la sección de *Hardware del servidor* apartado de *Análisis de soluciones*.

Se ha decidido utilizar como servidor el Dell PowerEdge 2950 Server. Cumple con todos los requisitos hardware y ofrece suficiente escalabilidad, ya que las características hardware de este servidor son muy elevadas.

Figura 43 Dell PowerEdge 2950 Server

A continuación, se especifican las características hardware del servidor Dell PowerEdge 2950 Server.

Concepto	Valor
Fabricante	DELL
Enrackable	Sí
Espacio en Us	2
Procesador	2 x Intel Xeon 4 Núcleos 2.66 GHz
Puertos de red	Intel® PRO/1000 PT, Gigabit Copper, PCI-E x4;
Almacenamiento interno	126 GB, aumentable a 1,8 TB

Memoria RAM	16 GB, aumentable a 32 GB
Fuente de alimentación	750 vatios

Tabla 14 Especificaciones DELL PowerEdge 2950 Server

Podemos ver que el servidor Dell PowerEdge 2950 Server cumple con todos los requisitos hardware establecidos en la sección de *Hardware del servidor* apartado de *Análisis de soluciones* para el despliegue de un servidor SIEM.

9.2.2 Hardware del sensor

Debido a los altos requerimientos de hardware y a las características de la red de la Diputación de Cádiz (Alto número de activos, red de, como máximo 1 Gbps,…) la máquina sobre la que se vayan a instalar los sensores SIEM debe cumplir, como mínimo, los requisitos dispuestos en la sección de *Hardware del sensor* apartado de *Análisis de soluciones*.

Para el despliegue de los sensores SIEM se van a utilizar dos máquinas:

- HP ProLiant DL320 G5p.
- HP ProLiant DL380 G4.

9.2.2.1 HP ProLiant DL320 G5p

Figura 44 HP ProLiant DL320 G5p

A continuación, se especifican las características hardware del servidor Dell PowerEdge 2950 Server.

Concepto	Valor
Fabricante	Hewlett-Packard (HP)
Enrackable	Sí
Espacio en Us	1
Procesador	Intel Xeon 2 Núcleos 2.13GHz
Puertos de red	Broadcom Corporation NetXtreme BCM5715 Gigabit Ethernet x2
Puertos PCI	PCI-X (133MHz, 3.3Volt)
Almacenamiento interno	126 GB, aumentable a 1 TB
Memoria RAM	6 GB, aumentable a 8 GB
Fuente de alimentación	400 vatios

Tabla 15 Especificaciones HP ProLiant DL320 G5p

Vemos que el servidor HP ProLiant DL320 G5p cumple con todos los requisitos hardware establecidos en la sección de *Hardware del sensor* apartado de *Análisis de soluciones* para el despliegue de un sensor SIEM.

9.2.2.2 HP ProLiant DL380 G4

Figura 45 HP ProLiant DL380 G4

A continuación, se especifican las características hardware del servidor HP ProLiant DL380 G4.

Concepto	Valor
Fabricante	Hewlett-Packard (HP)
Enrackable	Sí
Espacio en Us	1
Procesador	Intel Xeon 4 Núcleos 3.4GHz
Puertos de red	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet x2
Puertos PCI	PCI-X (133MHz, 3.3Volt)
Almacenamiento interno	126 GB, aumentable a 1 TB
Memoria RAM	6 GB, aumentable a 12 GB
Fuente de alimentación	575 vatios

Tabla 16 Especificaciones HP ProLiant DL380 G4

Vemos que el servidor HP ProLiant DL380 G4 cumple con todos los requisitos hardware establecidos en la sección de *Hardware del sensor* apartado de *Análisis de soluciones* para el despliegue de un sensor SIEM.

9.3 Localización de los sensores

Para que el sistema OSSIM que se va a desplegar en la red de la Diputación de Cádiz detecte todos los posibles ataques que se lleven a cabo, es necesario que dicho sistema OSSIM tenga la máxima visibilidad posible de todo el tráfico que se desea monitorizar. Para conseguir toda la visibilidad del tráfico y de los activos de la red de la Diputación de Cádiz, se deben desplegar cuantos sensores sean necesarios. Según lo establecido en el requisito R-01 en la entrevista con EPICSA, la zona prioritaria de monitorización es la zona frontera de la red.

En la zona frontera de la red de la Diputación de Cádiz aparecen diferentes tipos de conexiones:

- VPN sitio a sitio con el Ayto. de Puerto Real.
- VPNs sitio a sitio con las sedes remotas de la Diputación de Cádiz y Ayuntamientos de la provincia de Cádiz de municipios de menos de 20.000 habitantes.
- VPN sitio a sitio con la sede SS.CC de la Diputación de Cádiz.
- VPNs de acceso remoto para tele trabajadores de la Diputación de Cádiz.
- Acceso público a la red DMZ mediante direccionamiento IP proporcionado por RIPE.

- Conexiones a Internet de trabajadores de las sedes de la Diputación de Cádiz pertenecientes al anillo de red metropolitano.

Todas las conexiones VPN anteriormente expuestas que se establecen en la red de la Diputación de Cádiz son conexiones conocidas, es decir, los usuarios que la utilizan son usuarios conocidos y, a priori, son conexiones que no van a generar tráfico malicioso, por lo que no son prioridad para ser monitorizadas.

El acceso público a la red DMZ de la Diputación de Cádiz puede provocar que dicha red sufra ataques informáticos de cualquier parte del mundo, por lo que es una red con alta prioridad para ser monitorizada. De igual modo, las conexiones establecidas a Internet por trabajadores internos de la Diputación de Cádiz también pueden provocar ataques informáticos, por lo que dichas conexiones también deben ser monitorizadas.

A partir de ahora, el desarrollo de este apartado se va a centrar en los módulos de la zona frontera de la red de la Diputación de Cádiz denominados *PRESENCIA EN INTERNET y CONECTICVIDAD A INTERNET*, por lo que el esquema de red de la zona frontera de la red de la Diputación de Cádiz se verá simplificado.

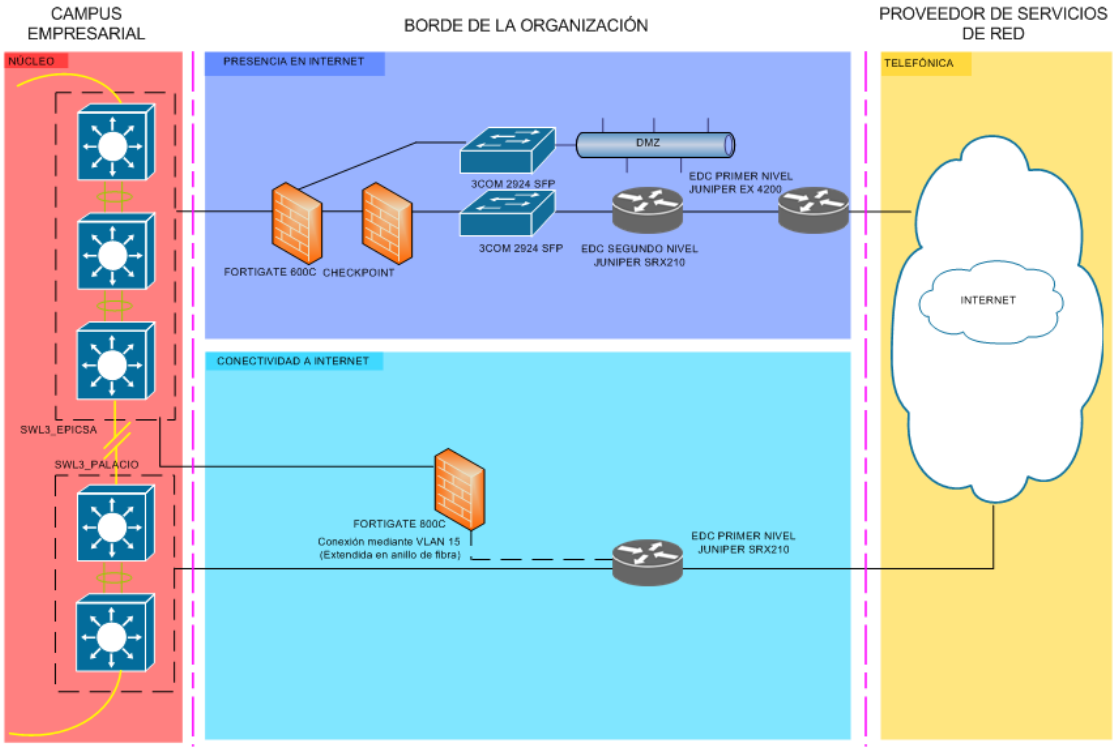


Figura 46 Zona frontera simplificada de la red de la Diputación de Cádiz

En primer lugar, vamos a analizar las diferentes procedencias que un posible ataque informático podría tener en estos módulos de la zona frontera de la red de la Diputación de Cádiz.

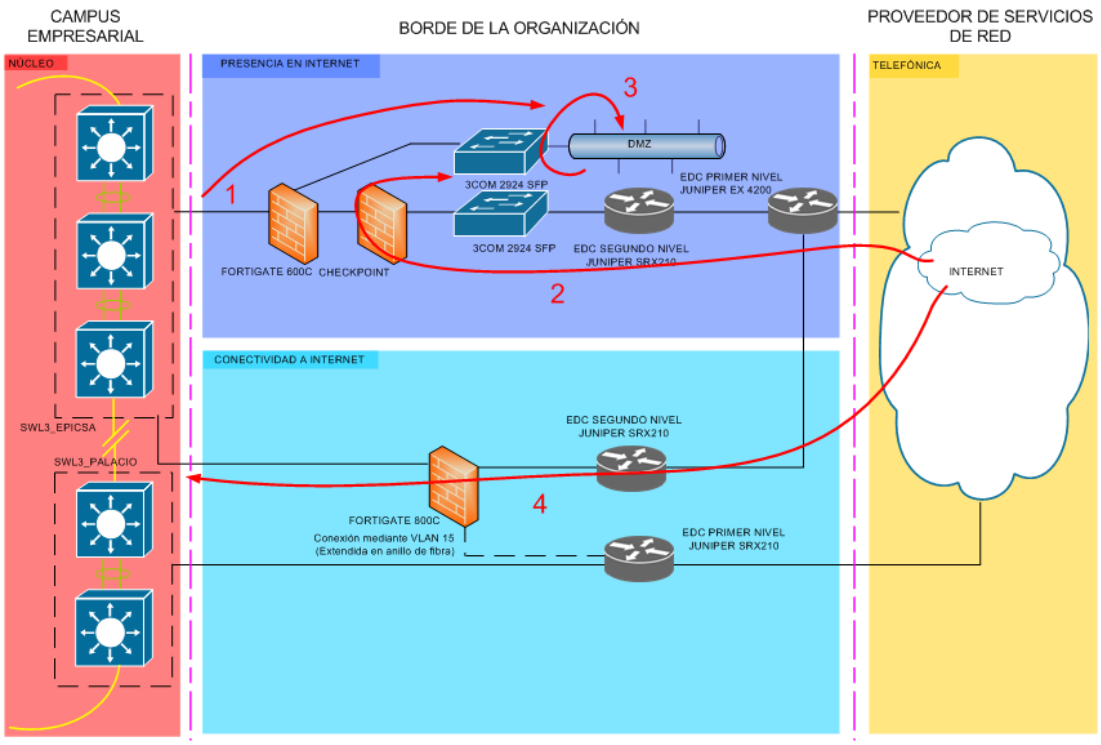


Figura 47 Posibles ataques a la zona frontera de la red de la Diputación de Cádiz

Los orígenes de los posibles ataques a la zona frontera de la red de la Diputación de Cádiz son los siguientes

- **Ataque 1**: Ataque interno a la red DMZ, ya sea por un virus en expansión en la red interna, por un usuario conocido con malas intenciones o por un atacante con acceso a la red interna.
- **Ataque 2**: Ataque externo a la red DMZ procedente de Internet.
- **Ataque 3**: Ataques entre propios activos de la red DMZ, ya sea por un virus en expansión en la red DMZ, por un usuario conocido con malas intenciones o por un atacante con acceso con privilegios a un activo de la red DMZ.
- **Ataque 4**: Ataque externo a la red interna procedente de internet debido a una conexión preestablecida por un usuario interno, por ejemplo, acceso a una web maliciosa, descarga de un ejecutable infectado, etc.

A modo de resumen, la procedencia y objetivo de esos ataques se puede observar en la siguiente tabla.

Ataque	Procedencia	Objetivo
1	LAN	DMZ
2	Internet	DMZ
3	DMZ	DMZ
4	Internet	LAN

Tabla 17 Posibles ataques en la zona frontera red de la Diputación de Cádiz

La localización de los sensores OSSIM a desplegar en la red de la Diputación de Cádiz debe asegurar que todo el tráfico de red generado por la aparición de alguno de los ataques expuestos anteriormente es monitorizado, por ello, la localización de los sensores OSSIM en la zona frontera de la red de la Diputación de Cádiz es la siguiente:

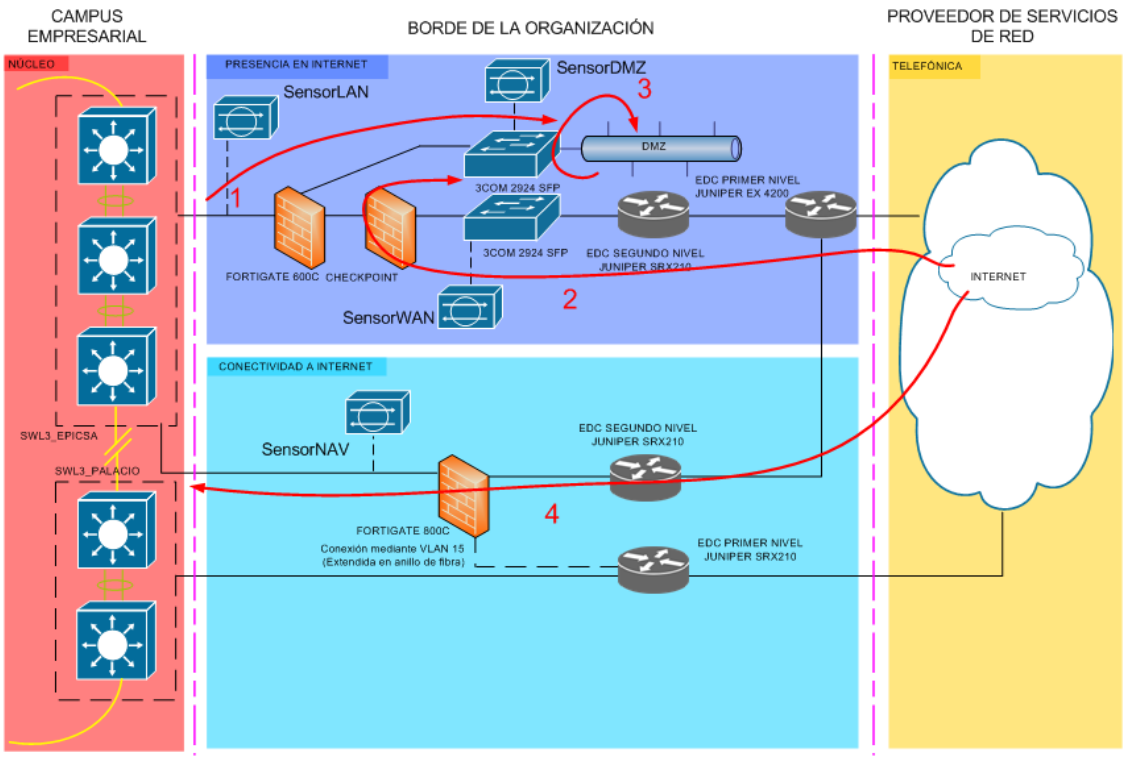


Figura 48 Localización de sensores en la zona frontera de la red de la Diputación de Cádiz

Es necesario que los sensores desplegados en la zona frontera de la red de la Diputación de Cádiz sean capaces de monitorizar todo el tráfico que transita la red para asegurar la correcta detección de ataques. Para ello, se realizarán las siguientes acciones, según el sensor desplegado.

- **SensorLAN** (detección de ataque 1). Se configura un puerto espejo en el clúster de conmutadores HP 5500 de núcleo, SWL3_EPICSA, que refleje todos los puertos de dicho clúster conectados al clúster de cortafuegos Fortigate 600C.
- **SensorWAN** (detección de ataque 2). Se configura un puerto espejo en el conmutador externo que refleja todo el tráfico entrante al clúster de cortafuegos Checkpoint.
- **SensorDMZ** (detección de ataque 3). Se configura un puerto espejo en el conmutador de la DMZ que refleje todos los puertos de conexión de servidores en la DMZ y los puertos de conexión al clúster de cortafuegos Fortigate 600C.
- **SensorNAV** (detección de ataque 4). Se configura un puerto espejo en el clúster de conmutadores HP 5500 de núcleo, SWL3_EPICSA, que refleje los puertos de conexión del clúster de cortafuegos Fortigate 800C.

Con el despliegue de sensores expuesto anteriormente se consigue monitorizar los módulos de la zona frontera de la red de la Diputación de Cádiz que más propensos son a sufrir un ataque y que, por tanto, tienen más prioridad en este proyecto.

9.4 Despliegue del SIEM

Tras lo expuesto en el análisis de soluciones con anterioridad, se debe decidir si dedicar una red fuera de línea a la red de interconexión del servidor OSSIM con los sensores que van a monitorizar las distintas secciones de la red de la Diputación de Cádiz.

Debido a que el sistema OSSIM se actualiza diariamente con motivo de la aparición de nuevas vulnerabilidades y patrones de ataques, además de la constante comunicación que el sistema OSSIM requiere con la comunidad AlienVault OTX sobre peligros emergentes, el sistema OSSIM debe permanecer constantemente conectado a Internet, por lo que la opción de una red fuera de línea no es factible en este caso.

Todas las conexiones que se van a utilizar para la gestión del servidor OSSIM y de los sensores se realizarán a través del clúster de conmutadores HP del módulo de *Granja de servidores y centro de datos* del área de *campus empresarial* de la red de la Diputación de Cádiz. Todo el tráfico que se transmitirá entre los servidores y los sensores se transportará sobre la VLAN ya configurada en la red de la Diputación de Cádiz para el transporte del tráfico de red de los servidores internos. Al estar conectados todos los componentes OSSIM a dicha VLAN de servidores, sus direcciones IP pertenecerán al bloque de direcciones asignado a los servidores: 172.22.0.0/19, siendo las siguientes las direcciones de cada uno de los componentes:

- **ServidorOSSIM**: 172.22.9.99
- **SensorDMZ**: 172.22.9.130
- **SensorWAN**: 172.22.9.53
- **SensorLAN**: 172.22.9.200
- **SensorNAV**: 172.22.5.99

El despliegue de los sensores, queda, por tanto, de la siguiente manera

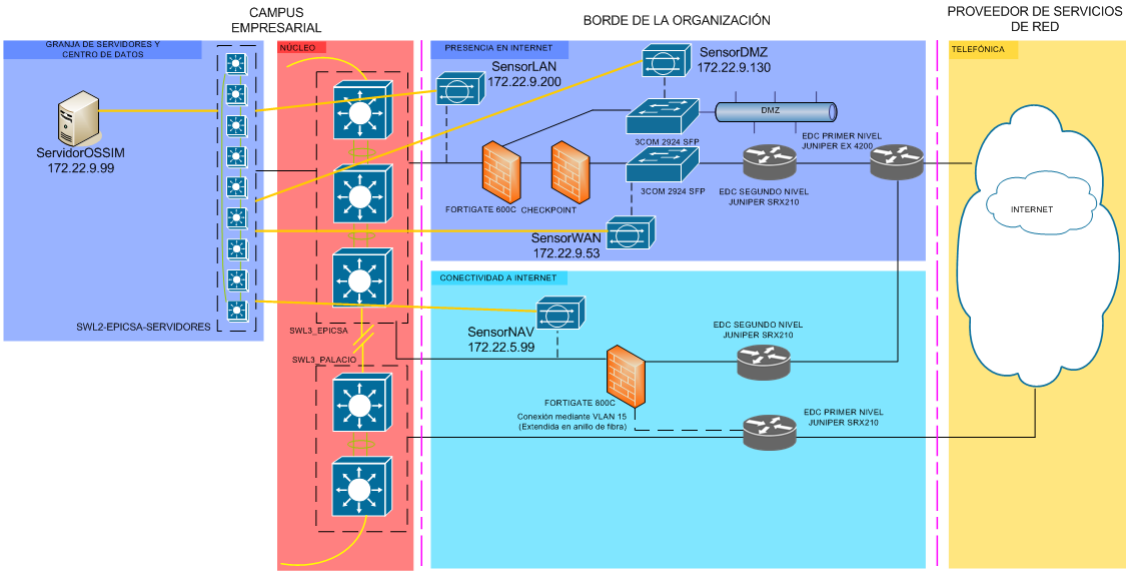


Figura 49 Despliegue del sistema OSSIM

Las máquinas elegidas para desplegar el sistema OSSIM son las siguientes:

- **ServidorOSSIM**: Dell PowerEdge 2925.
- **SensorDMZ**: HP ProLiant DL320 G5p.
- **SensorWAN**: HP ProLiant DL320 G5p.
- **SensorLAN**: HP ProLiant DL380 G4.
- **SensorNAV**: HP ProLiant DL380 G4.

El acceso a la interfaz web del servidor OSSIM se realiza a través de conexiones HTTPS y la conexión de administración a todos los componentes del sistema OSSIM se realiza a través de sesiones SSH.

Figura 50 Acceso por HTTPS al sistema OSSIM

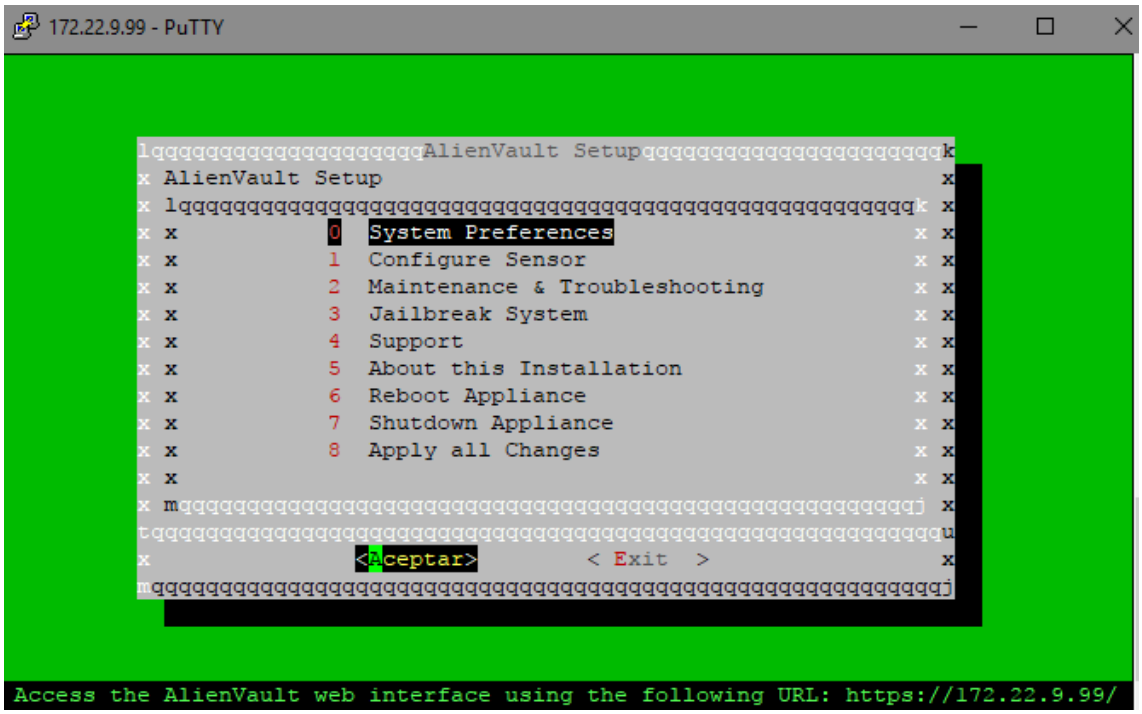


Figura 51 Acceso por SSH al sistema OSSIM

9.5 Configuración del SIEM

En el siguiente apartado y en sus sucesivas secciones se van a tratar los diferentes aspectos de la configuración del sistema OSSIM que más relevancia tienen en el desarrollo de este proyecto para el cumplimiento de los requisitos establecidos con EPICSA. También se expondrán ejemplos reales de configuración llevados a cabo en la red de la Diputación de Cádiz.

9.5.1 Detección de intrusiones

Tras la entrevista con EPICSA para la realización de este proyecto, se establecieron los requisitos R-01 y R-03 consistente en que el sistema OSSIM debe ser capaz de informar

ante alertas de seguridad producidas tanto en la red de la Diputación de Cádiz como en los activos de la Diputación de Cádiz con sistema operativo Windows.

Los dos siguientes apartados se centran en la solución adoptada en OSSIM para el cumplimiento de los requisitos R-01 y R-03, respectivamente.

9.5.1.1 Detección de intrusiones en red (NIDS)

El sistema OSSIM utiliza un detector de intrusiones en red llamado Suricata. Dicho sistema de detección de intrusiones en red utiliza un perfil de malo conocido para detectar ataques, ya que contiene almacenadas un conjunto de reglas que contrasta contra el tráfico que monitoriza para detectar patrones conocidos de ataques.

Suricata se ajusta a la perfección a la red de la Diputación de Cádiz, ya que su arquitectura está implementada de tal manera que soporte grandes cantidades de tráfico a analizar, debido a que soporta procesamiento multi-hilo. Las reglas que utiliza Suricata para detectar patrones de ataques se mantienen actualizadas diariamente por AlienVault y provienen de fuentes como la propia empresa y la comunidad Emerging Threats.

Por defecto, al desplegar el sistema OSSIM en un sensor que va a monitorizar tráfico de red, Suricata está activado por defecto en la interfaz que se configure como interfaz de monitorización. La instalación y configuración inicial de un sensor OSSIM se puede ver en el *Anexo C: Instalación del SIEM*.

En el servidor OSSIM desplegado en la red de la Diputación de Cádiz, toda la información relacionada con los eventos de seguridad detectados por Suricata se encuentra en

Analysis > Security Events (SIEM)

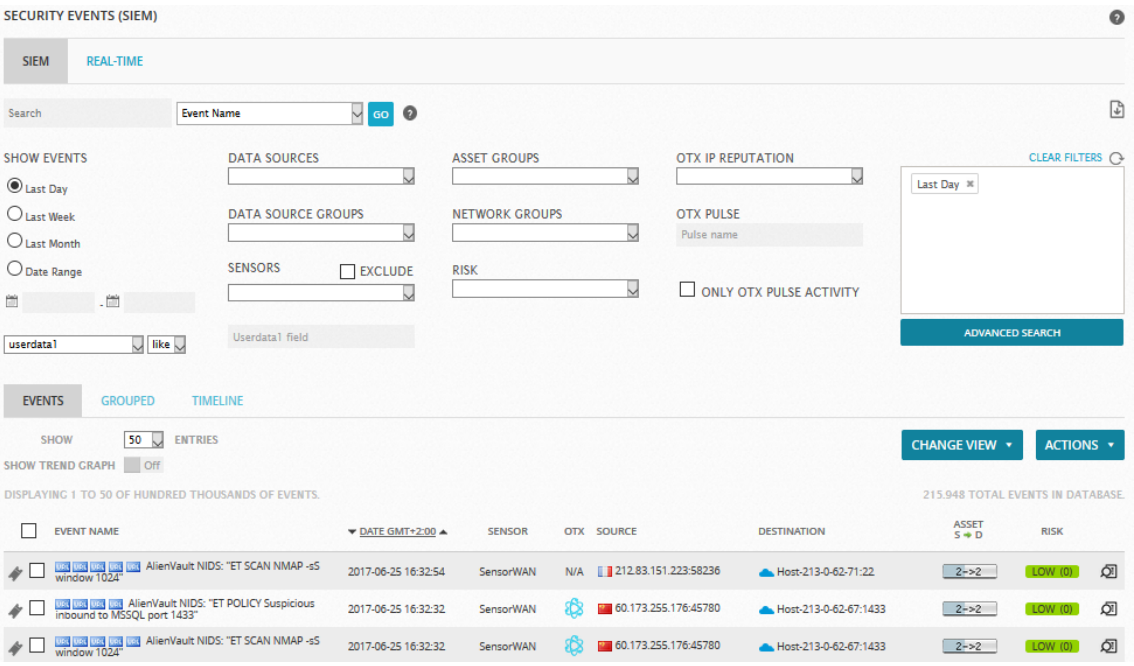


Figura 52 Sección de eventos de seguridad en OSSIM

En esta sección podemos visualizar todos los eventos generados por las diferentes fuentes de OSSIM, Suricata entre ellas, así como realizar búsquedas avanzadas y filtrar la

información. En esta página principal encontramos información importante sobre los eventos:

- Nombre del evento.
- Fecha de origen.
- Sensor que lo ha generado.
- Relación con AlienVault OTX
- Origen del evento.
- Destino del evento.
- Valor de importancia de los activos de origen y destino.
- Riesgo del evento

Si pulsamos en el icono de la izquierda en un evento, podemos visualizar información más concreta sobre el mismo, así como el paquete de red que ha generado la alerta y la regla de Suricata que lo ha detectado. El sistema OSSIM también nos ofrece la posibilidad de descargar dicho paquete en formato PCAP por si se desea analizar con una herramienta más especializada, como Wireshark, por ejemplo.

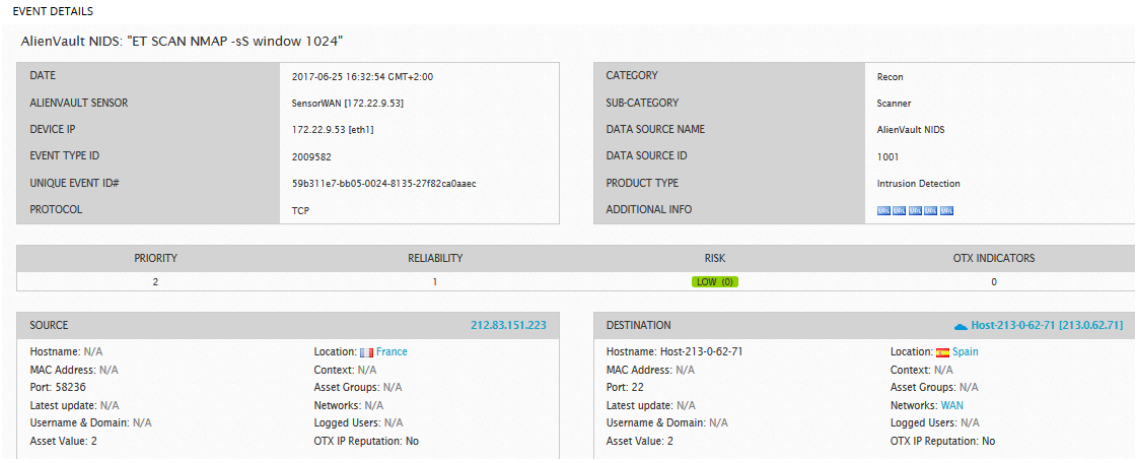


Figura 53 Información específica sobre activos relacionados en un evento de seguridad

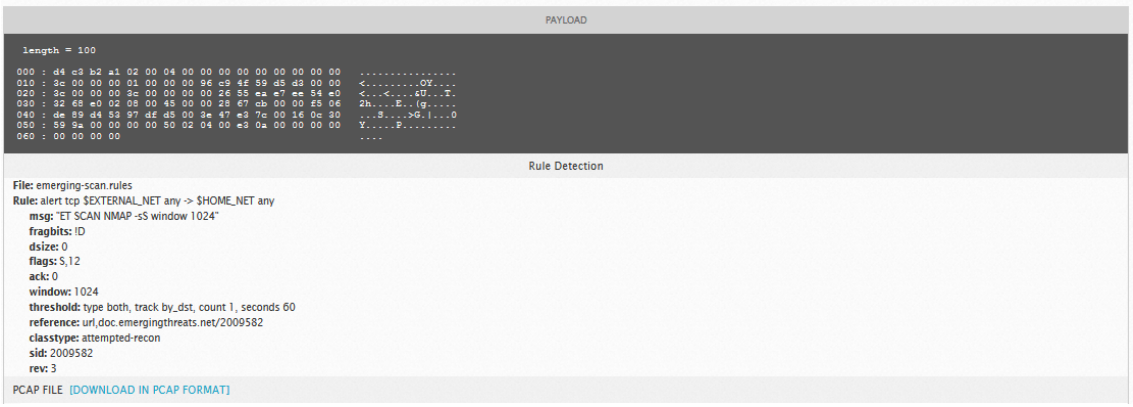


Figura 54 Información específica sobre el paquete que ha generado el evento de seguridad

Para que los sensores puedan detectar ataques entrantes en su red monitorizada y puedan detectar cualquier filtración de información hacia el exterior, hay que configurar en cada uno de los sensores OSSIM qué redes deben considerar como redes internas.

A continuación, se especifican las subredes de la Diputación de Cádiz que cada uno de los sensores va a monitorizar:

- SensorLAN: Todas las subredes clase C de las sedes de la Diputación de Cádiz pertenecientes al anillo de red metropolitano de la ciudad de Cádiz y la subred clase B de servidores internos.
- SensorWAN: Como el sensor se ha desplegado en una zona externa, tendrá la visibilidad de los dos bloques de direcciones públicas asignados a la Diputación de Cádiz.
- SensorDMZ: La subred bloque C perteneciente al módulo de presencia en Internet de la zona frontera de la red de la Diputación de Cádiz.
- SensorNAV: Todas las subredes clase C de las sedes de la Diputación de Cádiz pertenecientes al anillo de red metropolitano de la ciudad de Cádiz.

Para realizar esta configuración, debemos acceder a la consola de cada sensor mediante una sesión SSH y entrar en

Configure Sensor > Network CIDRs

En esta sección, introduciremos los bloques de subredes que cada uno de los sensores va a monitorizar. Se muestra la configuración específica del SensorLAN.

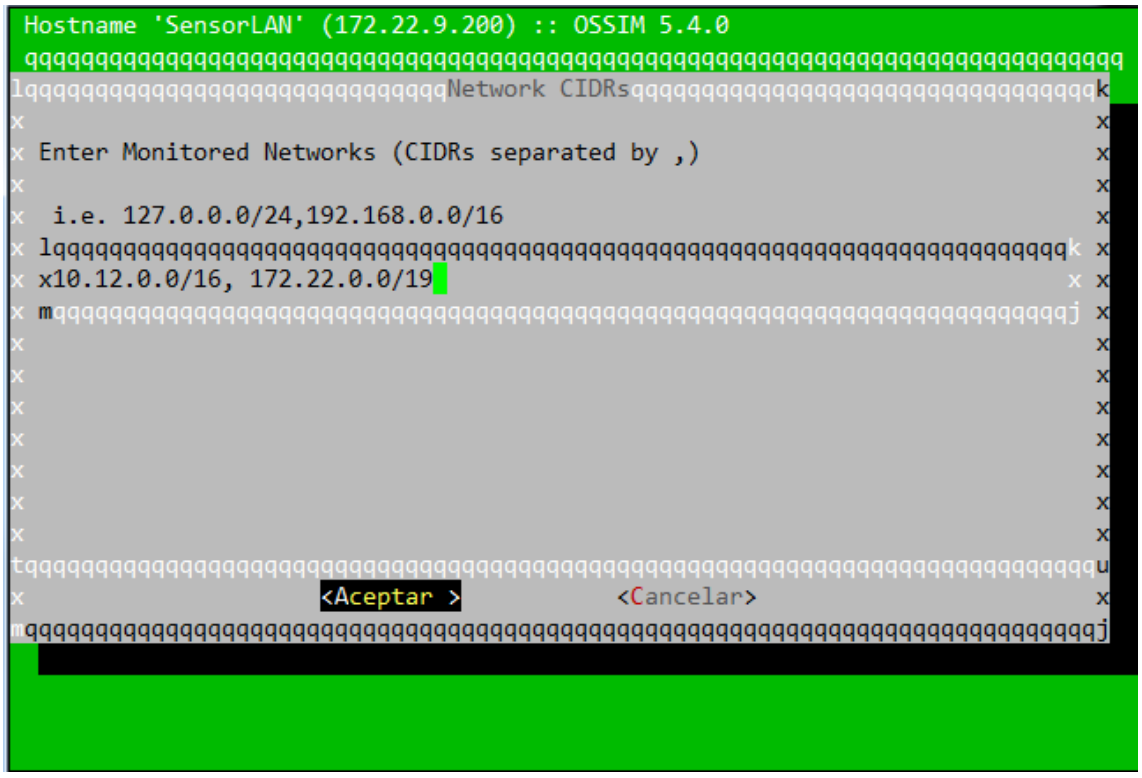


Figura 55 Configuración de redes a monitorizar por Suricata

Para que Suricata sea capaz de detectar ataques de tipo 3 (DMZ a DMZ) debemos definir una variable en el fichero de configuración de Suricata del SensorDMZ para que considere todas las direcciones IP como externas. Esto permite detectar ataques que en principio no salen de la red interna pero Suricata interpreta que salen a la red externa, para que se

puedan aplicar todos los patrones de ataques disponibles. Para realizar esta configuración, iniciamos una sesión SSH en el SensorDMZ y accedemos a

Jailbreak System

Una vez abierta la consola del sensor, debemos editar el fichero de configuración */etc/suricata/suricata.yaml* y alterar el valor de la variable:

EXTERNAL_NET: "!$HOME_NET" → EXTERNAL_NET: "any"

Tras esto, debemos reiniciar el servicio de Suricata, mediante el comando *service suricata restart*. Tras esto, nuestro SensorDMZ ya es capaz de detectar posibles ataques que se produzcan entre los servidores de la red DMZ de la Diputación de Cádiz.

Con toda esta información, el sistema OSSIM cumple con el requisito R-01 establecido tras la entrevista con EPICSA para la realización de este proyecto.

9.5.1.2 Detección de intrusiones en host (HIDS)

El sistema OSSIM utiliza un detector de intrusiones en host denominado OSSEC. OSSEC, al igual que Suricata utiliza un perfil de malo conocido basado en la comparación de eventos sucedidos en un activo con una serie de patrones o reglas que establecen eventos de seguridad.

El sistema OSSIM es capaz de desplegar de manera centralizada, mediante las credenciales de administración correspondientes, los agentes de OSSEC en todos los activos que se están monitorizando para que estos agentes reporten de toda la actividad generada y sea contrastada contra las reglas de OSSEC.

Todos los eventos de seguridad generados en la red de la Diputación de Cádiz relacionados con la detección de intrusiones en host por OSSEC se encuentran, al igual que los generados por Suricata, en

Analysis > Security Events (SIEM)

Para el cumplimiento del requisito R-03 establecido para la realización de este proyecto, es necesario que los agentes OSSEC estén instalados en todos los activos internos de la Diputación de Cádiz con sistema operativo Windows. Para ello, accedemos a

Environment > Assets & Groups

Seleccionamos todos los activos y accedemos a

Actions > Deploy HIDS

El sistema nos alertará de que, de todos los activos seleccionados, existen activos Linux, pero nos dará la opción de desplegar solo en equipos Windows, por lo que debemos elegir esa opción. Introducimos las credenciales de administración de los activos de la red de la Diputación de Cádiz con activos Windows y los agentes OSSEC comenzarán a desplegarse en todos los activos seleccionados.

Toda la información sobre los agentes OSSEC desplegados en la red de la Diputación de Cádiz se encuentra en

Environment > Detection

9.5.1.3 Sistema de alarmas

Para la generación de alarmas ante eventos de seguridad, el sistema OSSIM utiliza una fórmula que según diferentes parámetros establece un nivel de riesgo para dichos eventos. De esta manera, se tienen en cuenta diversos factores que nos ayudan a diferenciar un evento de seguridad que puede generar un falso positivo de un evento que merece más atención. La fórmula en cuestión es la siguiente:

$$Riesgo = (Valor\ del\ activo * Fiabilidad\ del\ evento * Prioridad\ del\ evento)/25$$

Según el valor de riesgo calculado, el sistema OSSIM lanzará una alarma con una prioridad u otra:

- Riesgo = 1, prioridad alta.
- Riesgo = 2, prioridad media.
- Riesgo ≥ 3, prioridad alta.

Cualquier evento relacionado con pulsos de OTX también generaran una alarma en el sistema OSSIM.

Todas las alarmas de seguridad se encuentran en

Analysis > Alarms

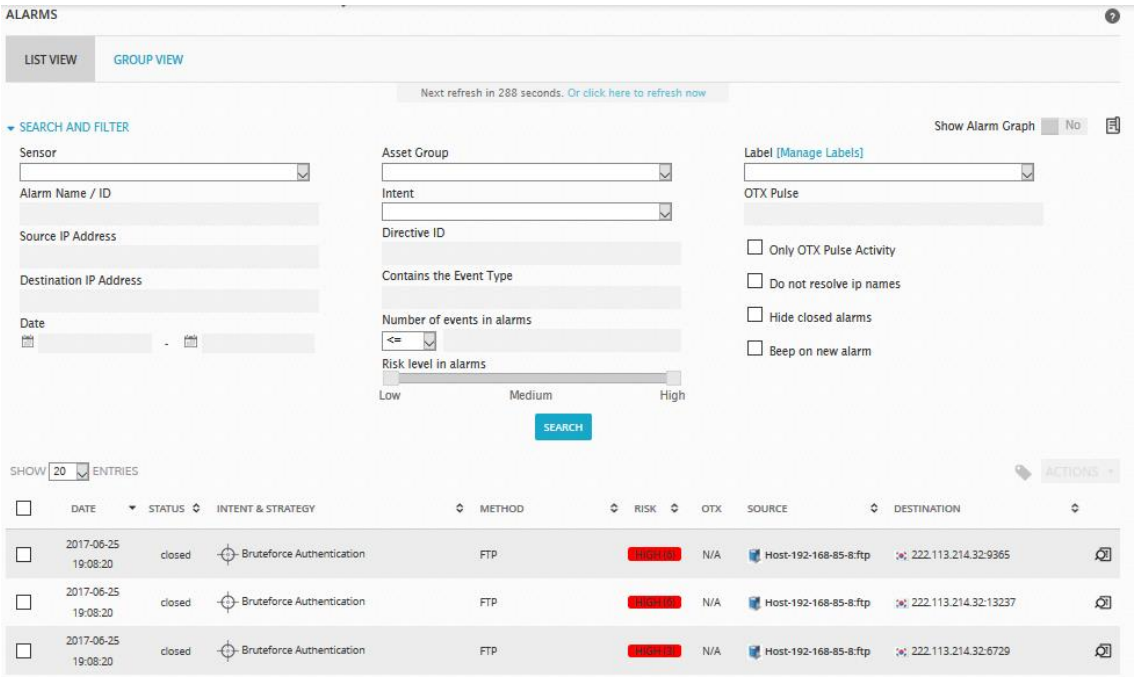


Figura 56 Sección de alarmas en OSSIM

En esta sección podemos ver un resumen de las alarmas generadas en el sistema OSSIM, así como realizar búsquedas y filtrado sobre las mismas. Si pulsamos en el icono de la izquierda de una alarma, accederemos a la información específica de cada alarma así como al evento o eventos que han generado dicha alarma.

9.5.2 Análisis de vulnerabilidades

Tras la entrevista con EPICSA para la realización de este proyecto, se estableció el requisito R-02, consistente en que el sistema OSSIM debe alertar sobre las vulnerabilidades encontradas en los activos de la red de la Diputación de Cádiz.

Debido al alto número de activos presentes en la red de la Diputación de Cádiz, los análisis de vulnerabilidades se realizarán a través de la red y, para conseguir la visibilidad máxima de todas las posibles vulnerabilidades de los equipos, todos los escáneres poseerán credenciales de administradores de los activos Windows de la Diputación de Cádiz, por lo que dichos escáneres se realizarán con perspectiva de administrador.

El sistema OSSIM debe analizar las vulnerabilidades en los activos presentes en todas y cada una de las subredes de la Diputación de Cádiz que se están monitorizando:

- Subredes clase C pertenecientes a las sedes de la Diputación de Cádiz pertenecientes al anillo de red metropolitano.
- Subred clase C perteneciente a la red DMZ de la Diputación de Cádiz.

Además, se configurará un escáner de vulnerabilidades en la red de servidores internos de EPICSA, cuyos activos se encuentran en los bloques de direcciones 172.22.8.0/24 y 172.22.9.0/24, respectivamente. Para controlar las vulnerabilidades que puedan aparecer en los dispositivos de red, se realizará un escáner de vulnerabilidades de la red de gestión de conmutadores del anillo de red metropolitano de la Diputación de Cádiz, cuya subred es la 172.32.1.0/24. Cada semana se repetirán todos los escáneres debido al alto grado de vulnerabilidades que aparecen semanalmente, de tal manera que la información sobre las vulnerabilidades presentas y/o vulnerabilidades a buscar sea la más actualizada posible. OpenVAS actualiza diariamente su base de vulnerabilidades y análisis de diversas fuentes como CVE.

La planificación semanal de los escáneres de vulnerabilidades se ha configurado de tal manera que nunca coincidan temporalmente dos escáneres de vulnerabilidades, debido al alto nivel de tráfico que generan dichos escáneres.

Sensores: DMZ WAN LAN NAV

Día / Hora	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo
8:00 -- 9:00							
9:00 -- 10:00	EPICSA PB	RESIDENCIA	PALACIO 1	PALACIO 3	EUROPA		
10:00 -- 11:00	EPICSA T	IEDT	PALACIO 2	PALACIO 4	RIVADAVIA		
11:00 -- 12:00	EPICSA PP	S. ANTONIO	ROMA	CAPUCHINOS	GLORIETA		
12:00 -- 13:00	EPICSA AF	ANTONIO L.	GUADAL.	AG. ENER.	MEDIA MB		
13:00 -- 14:00							
14:00 -- 15:00							
15:00 -- 16:00							
16:00 -- 17:00					Servidores 8	ANILLO	
17:00 -- 18:00					Servidores 9	DMZ	
18:00 -- 19:00							
19:00 -- 20:00							
20:00 -- 21:00							

Tabla 18 Planificación semanal del escáner de vulnerabilidades

Los escáneres de vulnerabilidades se lanzan a través de las interfaces de gestión de los sensores por lo que, independientemente de qué subred estén monitorizando a través de la interfaz de monitorización, todos los sensores pueden escanear cualquier subred.

En el sistema OSSIM, Toda la información relacionada con los escáneres de vulnerabilidades configurados y las vulnerabilidades encontradas en los activos se encuentra en

Environment > Vulnerabilities

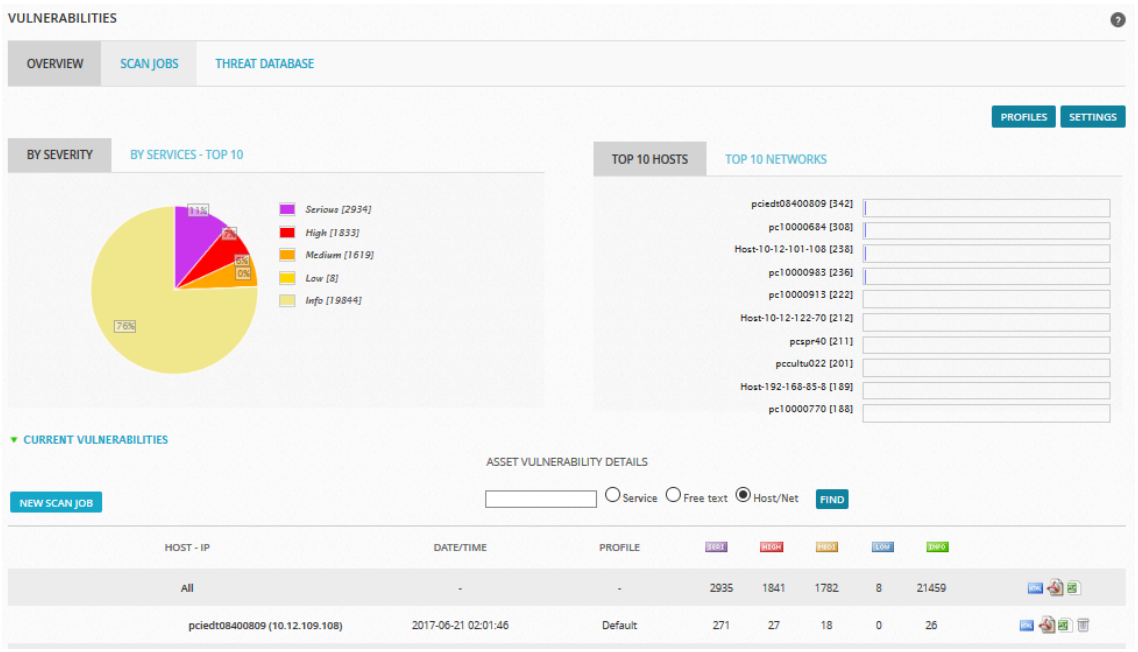


Figura 57 Sección principal sobre análisis de vulnerabilidades en OSSIM

En concreto, la información sobre los escáneres de vulnerabilidades configurados en el sistema OSSIM se encuentra en

Environment > Vulnerabilities > Scan Jobs

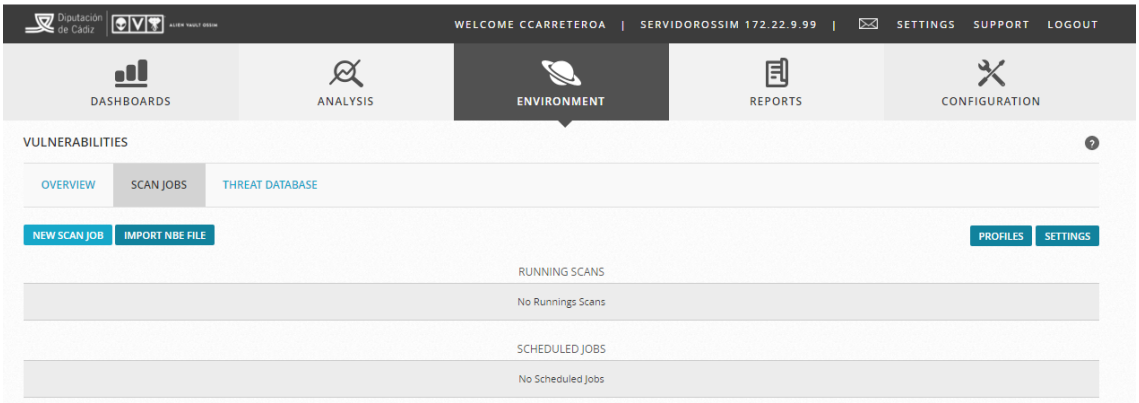


Figura 58 Sección de escáneres de vulnerabilidades

Primero debemos configurar las credenciales de administrador de los equipos Windows de la Diputación de Cádiz para que el sistema OSSIM pueda analizar los activos internamente. Para ello, accedemos a SETTINGS y configuramos las credenciales en la sección CREDENTIALS

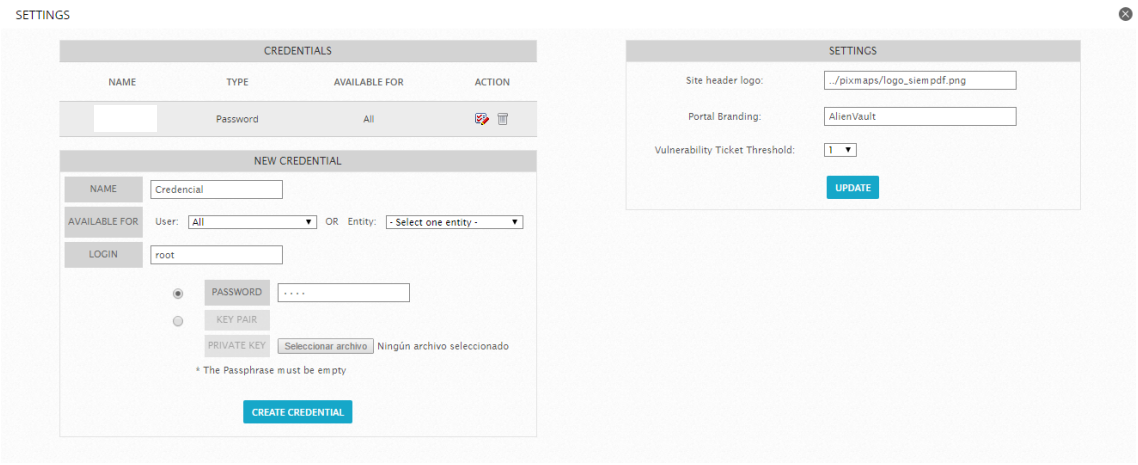


Figura 59 Configuración de credenciales de administrador para el escáner de vulnerabilidades

Nota: Se ha omitido el nombre del usuario por motivos de confidencialidad.

Una vez que hemos configurado las credenciales de administración, ya podemos configurar los escáneres de vulnerabilidades. En este caso en concreto, se muestra la configuración para el escáner de vulnerabilidades de la subred EPICSA PLANTA BAJA (EPICSA PB), siendo esta idéntica para el resto de subredes a escanear.

Para realizar la configuración, pulsamos el botón de NEW SCAN JOB e introducimos la configuración del escáner de vulnerabilidades.

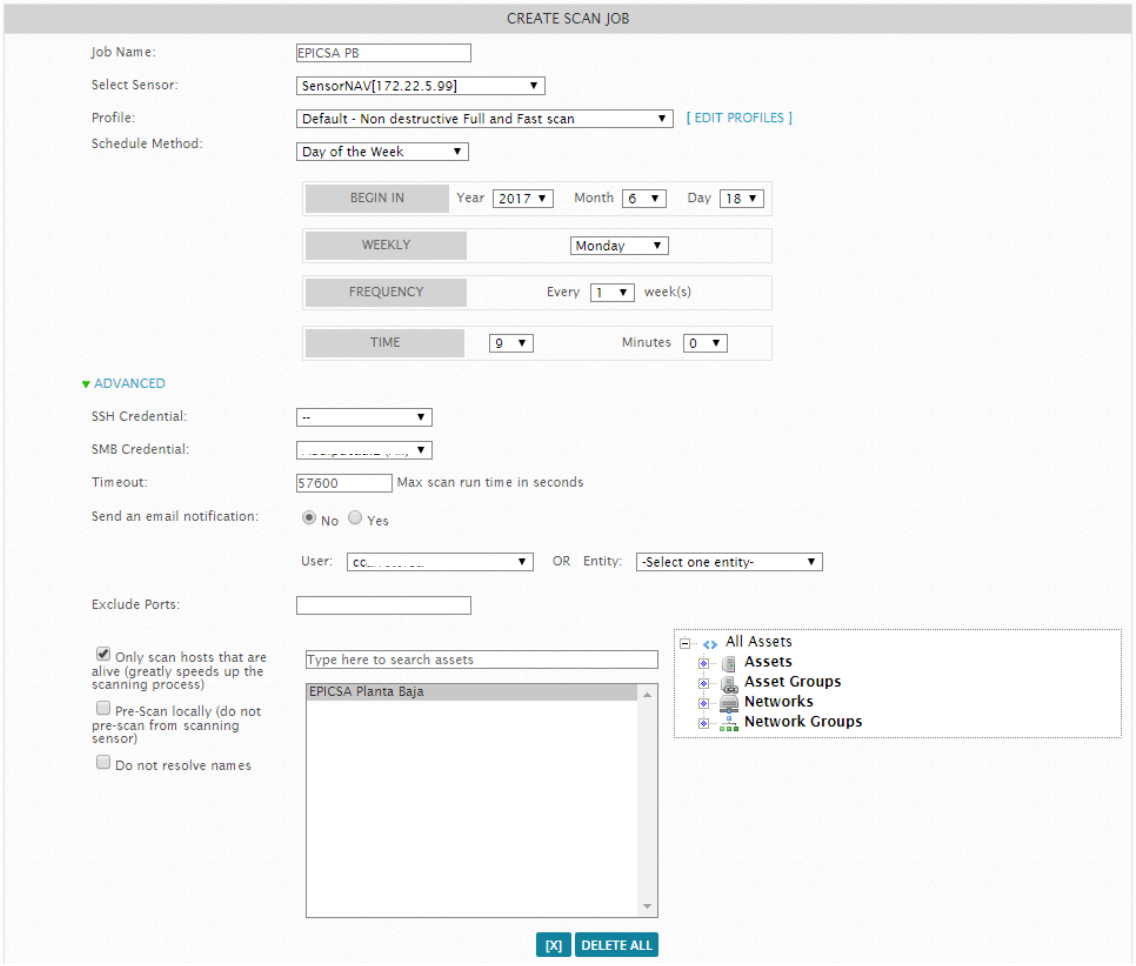


Figura 60 Nuevo escáner de vulnerabilidades

Nota: Se ha omitido el nombre del usuario por motivos de confidencialidad.

En esta sección podemos configurar parámetros como:

- Nombre del escáner.
- Sensor OSSIM que realizará el análisis.
- Perfil del escáner.
- Planificación temporal del escáner.
- Credenciales SSH o SMB de administración.
- Usuario a cargo del escáner.
- Redes o activos a escanear.
- Escanear todas las direcciones IP de la red o sólo los activos que están activos

Una vez que hayamos introducido la información, el sistema OSSIM verificará que es correcta y podremos activar el escáner.

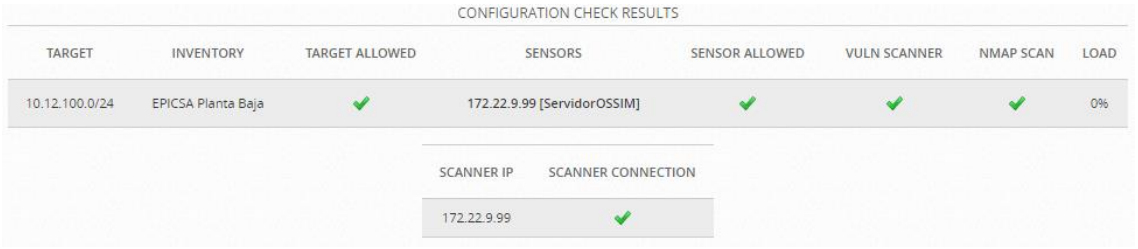


Figura 61 Verificación de configuración de escáner de vulnerabilidades

Ahora podremos ver que nuestro escáner está activo y a la espera de su hora de lanzamiento.

Figura 62 Verificación de lanzamiento de escáner de vulnerabilidades

En el sistema OSSIM es importante elegir qué tipo de perfil queremos configurar para nuestro escaneo. Un perfil de escáner de vulnerabilidades en OSSIM define que vulnerabilidades se van a analizar, que acciones realizar cuando se encuentran las vulnerabilidades (informar o intentar apagar el activo) y que agresividad tendrá el escáner (lento o rápido) en lo referente a la cantidad de tráfico de red que genera dicho escáner en un determinado espacio de tiempo. Por defecto, el sistema OSSIM cuenta con tres perfiles predeterminados:

- Deep. Se escanean todas las vulnerabilidades, sin tests destructivos y con una agresividad baja. Este escáner es ideal para redes que soportan poca carga de trabajo.
- Default. Se escanean todas las vulnerabilidades, sin test destructivos y con una agresividad normal. Este escáner es ideal para redes que soportan alta carga de trabajo.
- Ultimate. Se escanean todas las vulnerabilidades, con tests destructivos y con una agresividad alta. Este escáner es ideal para redes que soportan mucha carga de trabajo y para expertos en seguridad que quieren ver hasta que punto es capaza de aguantar una red una alta carga de trabajo y ver que activos podrían sufrir denegaciones de servicio.

Los escáneres configurados en las subredes de la Diputación de Cádiz seguirán el perfil Default, ya que la red de la Diputación de Cádiz puede soportar la carga de trabajo, se desea que se analicen todas las vulnerabilidades, pero no se desea que el escáner provoque denegaciones de servicio en los activos mediante tests destructivos.

Tras configurar todos los escáneres de vulnerabilidades en la red de la Diputación de Cádiz, podemos ver como aparecen listados en la sección de escáneres de vulnerabilidades programados.

NAME	SCHEDULE TYPE	TIME	NEXT SCAN	STATUS	ACTION
DMZ	Weekly	17:00:00	2017-07-01 17:00:00	Enabled	
ANILLO	Weekly	16:00:00	2017-07-01 16:00:00	Enabled	
SERVIDORES 9	Weekly	17:00:00	2017-06-30 17:00:00	Enabled	
SERVIDORES 8	Weekly	16:00:00	2017-06-30 16:00:00	Enabled	
MEDIA MB	Weekly	12:00:00	2017-06-30 12:00:00	Enabled	
GLORIETA	Weekly	11:00:00	2017-06-30 11:00:00	Enabled	
RIVADAVIA	Weekly	10:00:00	2017-06-30 10:00:00	Enabled	
EUROPA	Weekly	09:00:00	2017-06-30 09:00:00	Enabled	
AG. ENER.	Weekly	12:00:00	2017-06-29 12:00:00	Enabled	
CAPUCHINOS	Weekly	11:00:00	2017-06-29 11:00:00	Enabled	
PALACIO 4	Weekly	10:00:00	2017-06-29 10:00:00	Enabled	
PALACIO 3	Weekly	09:00:00	2017-06-29 09:00:00	Enabled	
GUADAL	Weekly	12:00:00	2017-07-12 12:00:00	Enabled	
ROMA	Weekly	11:00:00	2017-07-05 11:00:00	Enabled	
PALACIO 2	Weekly	10:00:00	2017-07-05 10:00:00	Enabled	
PALACIO 1	Weekly	09:00:00	2017-07-05 09:00:00	Enabled	
ANTONIO L.	Weekly	12:00:00	2017-07-04 12:00:00	Enabled	
S. ANTONIO	Weekly	11:00:00	2017-07-04 11:00:00	Enabled	
IEDT	Weekly	10:00:00	2017-07-04 10:00:00	Enabled	
RESIDENCIA	Weekly	09:00:00	2017-07-04 09:00:00	Enabled	
EPICSA AF	Weekly	12:00:00	2017-07-24 12:00:00	Enabled	
EPICSA PP	Weekly	11:00:00	2017-07-24 11:00:00	Enabled	
EPICSA T	Weekly	10:00:00	2017-07-17 10:00:00	Enabled	
EPICSA PB	Weekly	09:00:00	2017-07-17 09:00:00	Enabled	

Figura 63 Lista completa de escáneres de vulnerabilidades configurados

Cuando un escáner se lleve a cabo y finalice, podremos encontrar los resultados en una sección denominada ALL SCANS. Por ejemplo, veamos el resultado de un escáner de vulnerabilidades realizado a los activos de la sede CAPUCHINOS. Para visualizar dicho resultado, disponemos de varias opciones:

- Visualización en una página web.
- Exportación en PDF.
- Exportación a archivo para visualización en Microsoft Excel.
- Exportación a archivo con extensión NBE.

Desde esta lista de visualización también podemos borrar los resultados del escáner, relanzarlo, o asignárselo a otro usuario del sistema OSSIM.

Figura 64 Opciones de visualización de resultados de escáner de vulnerabilidades

En este caso, vamos a ver los resultados en una página HTML.

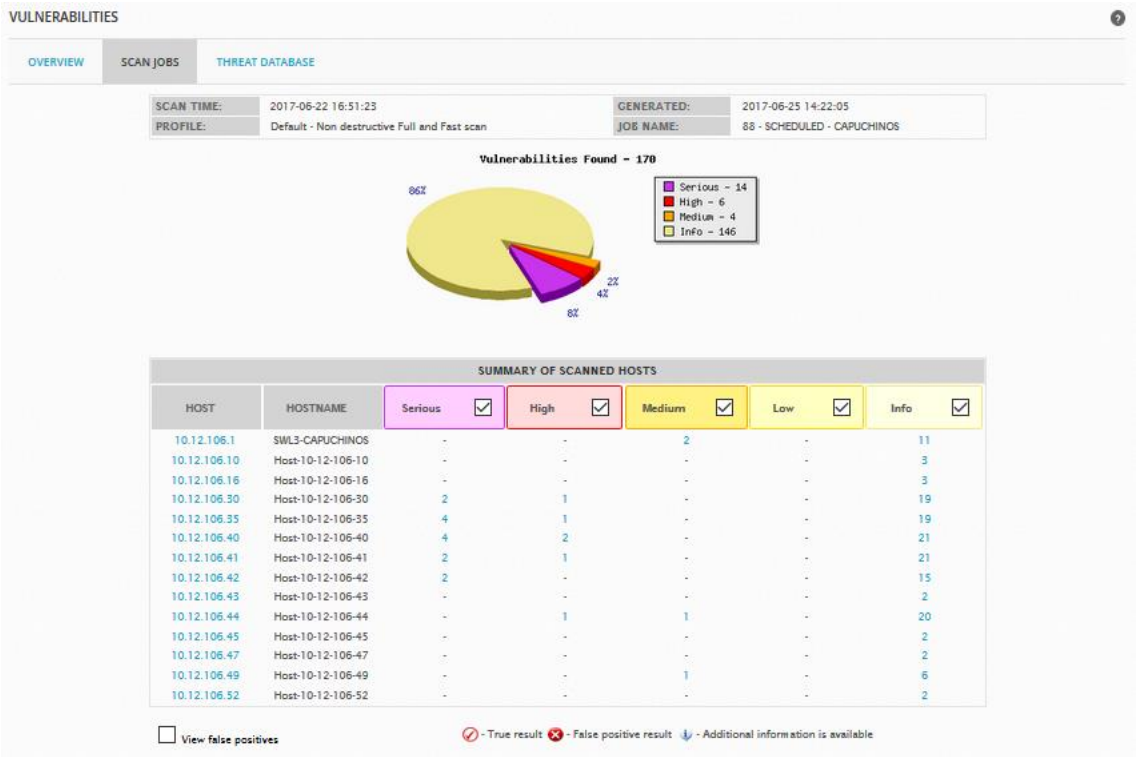


Figura 65 Resultados en HTML de un escáner de vulnerabilidades

En la primera sección podemos ver una tabla con los activos pertenecientes a la red en la que se ha realizado el escáner y las diferentes vulnerabilidades encontradas en cada activo clasificadas en cuatro niveles de riesgo, de más alto a más bajo: Serious, High, Medium, Low. El quinto nivel (Info) es información que el escáner ha recabado sobre el activo escaneado. Podemos elegir mostrar todos los niveles de importancia, un grupo de ellos, o uno solo. Si pulsamos sobre un activo, la página se moverá directamente a la sección donde se detallan al completo todas las vulnerabilidades de dicho activo.

En la página central de OSSIM sobre las vulnerabilidades encontramos un resumen global sobre qué activos escaneados poseen más vulnerabilidades y disponemos de un buscador de activos que nos permite mostrar las últimas vulnerabilidades encontradas en un activo determinado

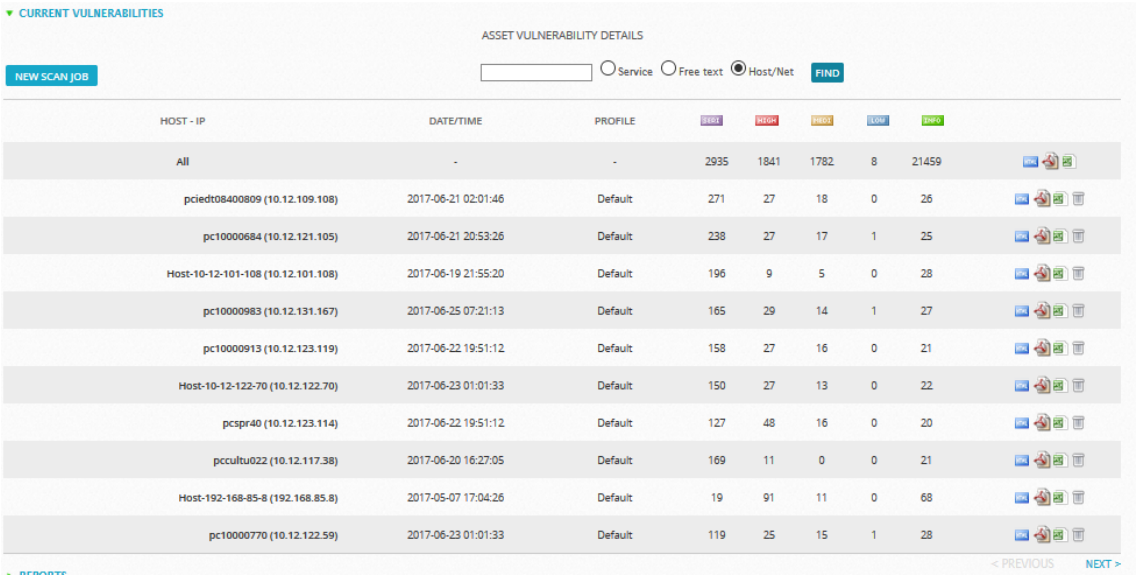


Figura 66 Buscador de activos para mostrar sus vulnerabilidades

9.5.3 Información administrativa

Tras la entrevista con EPICSA para la realización de este proyecto, se estableció el requisito R-04, consistente en que el sistema SIEM debe ofrecer la posibilidad de presentar información administrativa de la red.

El sistema OSSIM ofrece la posibilidad de tener un inventario con información sobre las redes monitorizadas por dicho sistema y un inventario con información sobre los activos pertenecientes a las redes monitorizadas. Además, el sistema OSSIM es capaz de recibir y presentar información sobre estadísticas de uso de la red, así como, las diferentes sesiones que se establecen a lo largo del tiempo

9.5.3.1 Redes con activos a monitorizar

Para el agrupamiento y gestión eficaz de los activos pertenecientes a la red de la Diputación de Cádiz, es necesario configurar en el sistema OSSIM todas las redes de la Diputación de Cádiz cuyos activos vayan a tener visibilidad en los enlaces monitorizados por los sensores desplegados. Según el sensor desplegado en la zona frontera de la red de la Diputación de Cádiz, las redes con visibilidad en el tráfico de red son las establecidas en la sección de *Detección de Intrusiones en Red (NIDS)*. Para añadir todas estas redes en al sistema OSSIM, debemos acceder a

Environment > Assets & Groups > Networks > Add Network

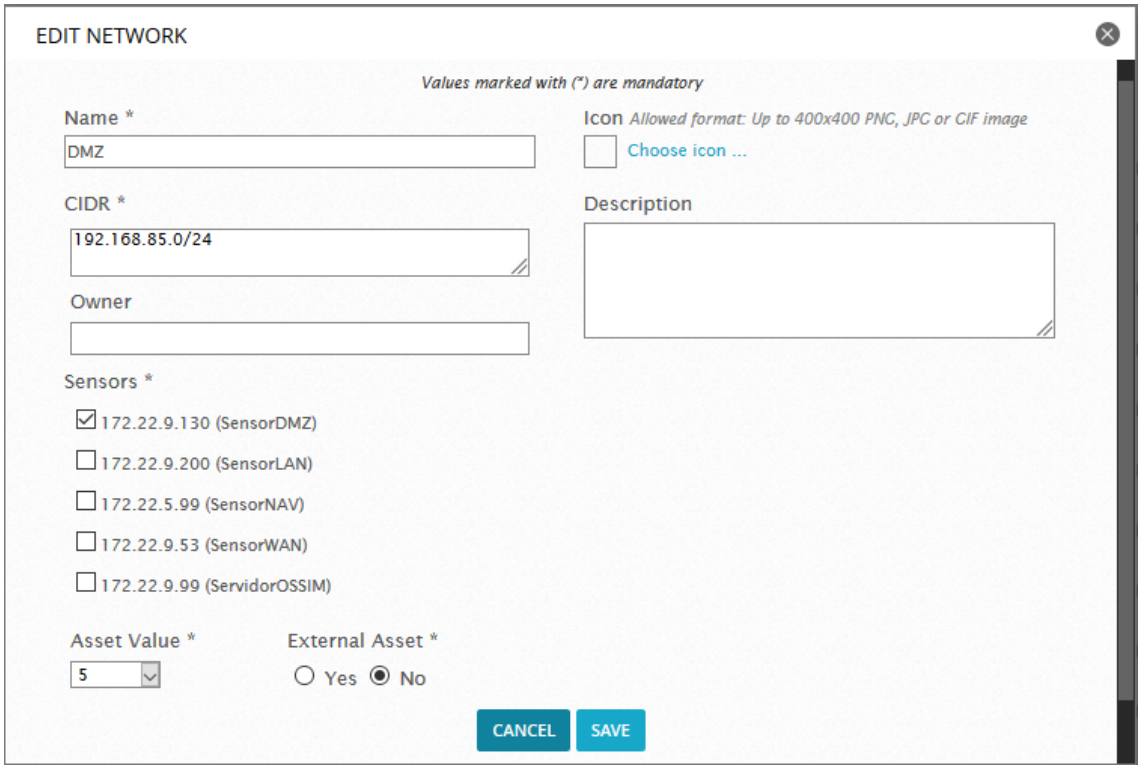


Figura 67 Inserción de una red monitorizada en el sistema OSSIM

En la adición de una subred podemos configurar datos como:

- Bloque de direcciones IP.
- Sensor que va a tener visibilidad de la subred.
- Valor de los activos pertenecientes a la subred.
- Etc.

Tras realizar todas estas acciones con todas las subredes cuyos activos van a generar tráfico de red y se desean monitorizar, disponemos de toda esa información en:

Environment > Assets & Groups > Networks

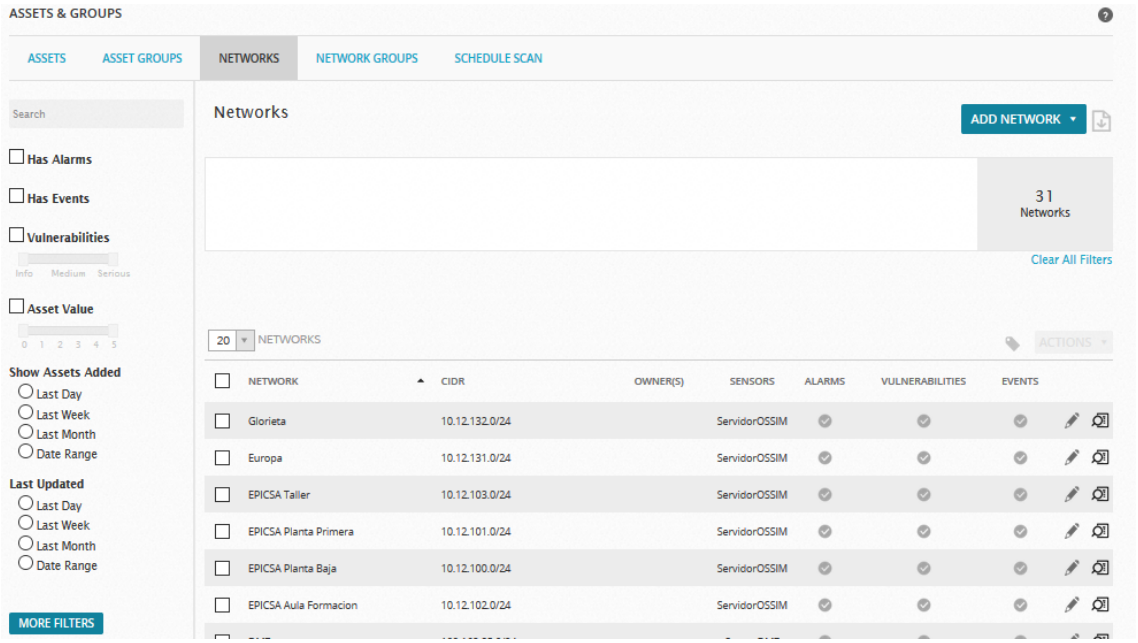


Figura 68 Sección de información de subredes monitorizadas en OSSIM

Dentro de dicha sección, además del listado de las redes configuradas, podemos filtrar y buscar en dicha lista según diferentes criterios, como mostrar redes cuyos activos han generado alarmas de seguridad, mostrar redes en cuyos activos se han detectado vulnerabilidades, mostrar redes en las que se han añadido activos recientemente, etc.

9.5.3.2 Listado de activos

Tal y como se ha especificado anteriormente, el sistema OSSIM mantiene un inventario de todos los activos de la red o las redes que se están monitorizando. Dicha información incluye:

- Dirección IP y dirección MAC.
- Sistema operativo.
- Puertos abiertos, con los servicios correspondientes.
- Vulnerabilidades encontradas.
- Alarmas de seguridad relacionadas.
- Eventos de seguridad relacionados.
- Estado de actividad (apagado/encendido).
- Nivel de importancia del activo.
- Etc.

Todo lo relacionado con la información e inventario de activos de la red monitorizada se encuentra disponible en

Environment > Assets & Groups

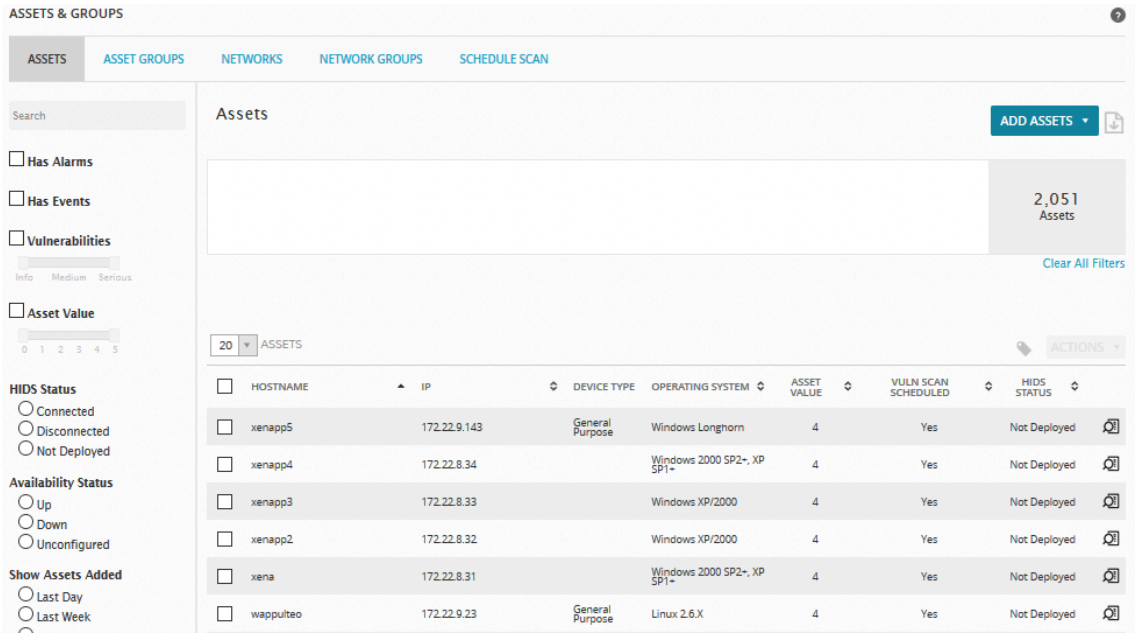


Figura 69 Sección de inventario de activos en OSSIM

Para añadir activos en el sistema OSSIM, tenemos varias opciones, disponibles en el botón ADD ASSETS:

- Añadirlos manualmente.
- Importar un listado de activos desde un archivo con extensión CSV.
- Escanear una red en busca de activos.
- Guardar nuevos activos que se hayan detectado en eventos de seguridad.

Para la adición de los activos de las subredes de la Diputación de Cádiz en el sistema OSSIM, se realizaron escaneos en todas las subredes configuradas anteriormente. Por ejemplo, se muestra la configuración del escaneo de activos realizado en la subred DMZ.

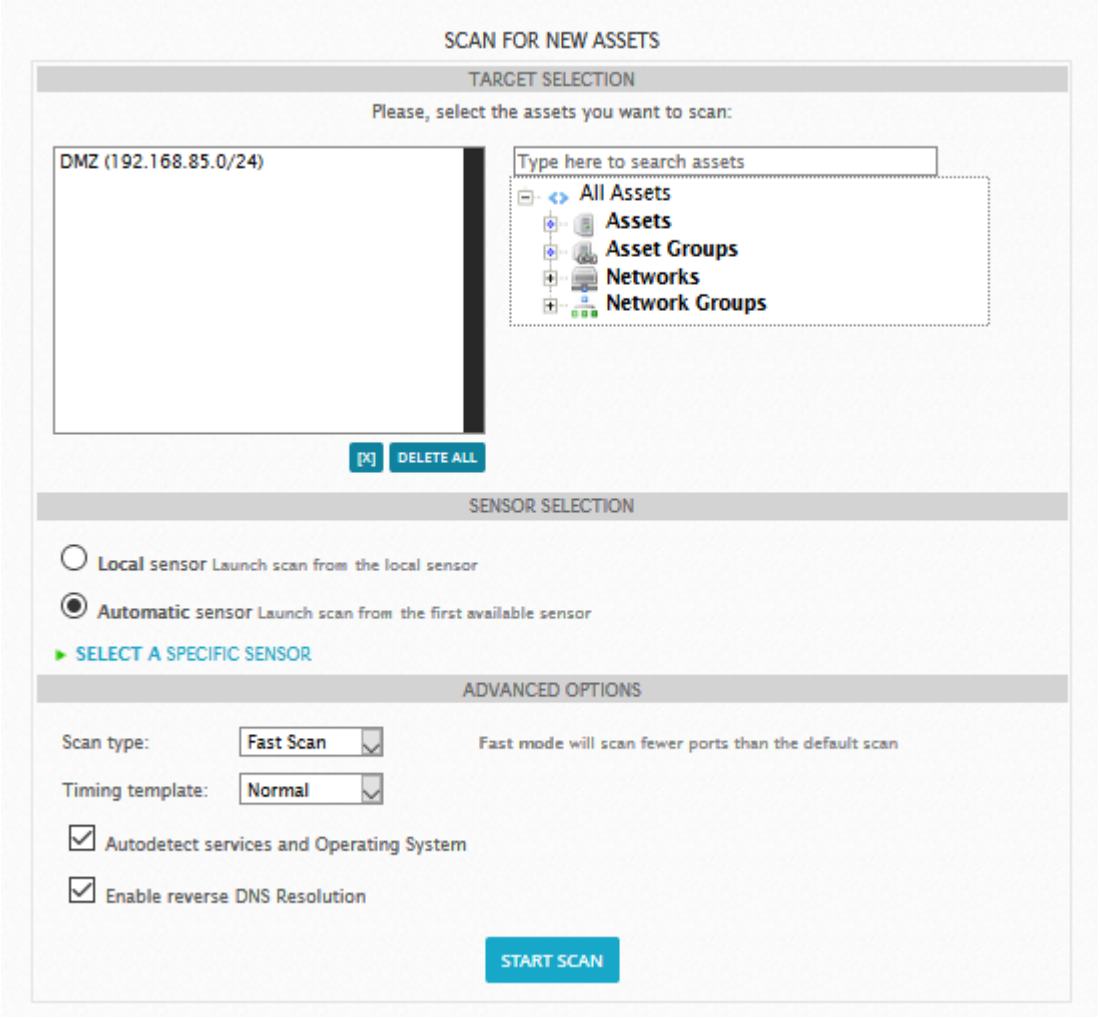


Figura 70 Configuración de escáner de activos en la red DMZ en OSSIM

Para configurar un escáner, se deben elegir parámetros como:

- Objetivo del escáner: una o varias subredes a la vez
- Sensor OSSIM desde el que se va a lanzar el escáner
- Opciones avanzadas, como el tipo de escaneo, la plantilla de tiempo, resolución DNS y detección de sistemas operativos y servicios.

Tal y como se ha especificado anteriormente, se realizaron escáneres en todas las subredes mencionadas en la sección anterior.

Una vez que se han configurado las redes a monitorizar y se han escaneado dichas redes en busca de activos, si el sistema OSSIM detecta un evento de seguridad relacionado con un activo cuya dirección IP pertenece a un bloque de direcciones perteneciente a una red monitorizada pero dicho activo no estaba previamente guardado en el sistema, OSSIM lo guarda automáticamente. Esta acción tiene mucha importancia para redes cuya asignación de direcciones se basa en el protocolo DHCP.

9.5.3.3 Estadísticas de uso de la red

La recolección de estadísticas de uso de la red en el sistema OSSIM se basa en la recolección de reportes periódicos generados por terceros en base al tráfico de red que los

sensores monitorizan. Esta recolección también puede proceder de otros dispositivos de red, como conmutadores, routers o cortafuegos.

Para que el sistema OSSIM contenga información sobre las estadísticas de uso de la red de la Diputación de Cádiz, vamos a configurar cada uno de los sensores para que envíen reportes periódicos de todo el tráfico que está monitorizando cada uno de ellos.

La arquitectura de funcionamiento de todo el envío y recepción de reportes es el siguiente

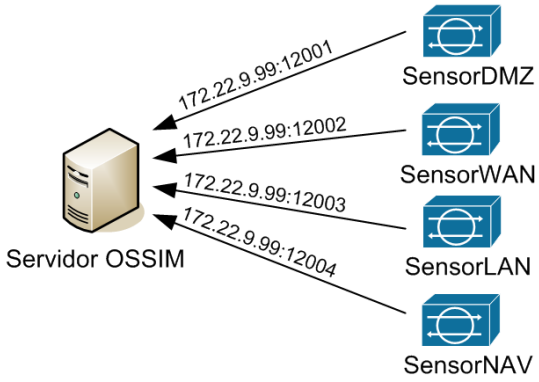


Figura 71 Envío y recepción de estadísticas de red

Como ejemplo, se va a exponer la configuración a realizar para activar el envío y recepción de estadísticas de red generadas en el SensorDMZ, siendo dicha configuración idéntica en cada uno de los demás sensores.

Primero, debemos iniciar una sesión a través de SSH en el sensor SensorDMZ en su dirección IP 172.22.9.130. Una vez iniciada dicha conexión y habiendo introducido correctamente las credenciales del usuario, accedemos a

Configure Sensor > Enable Netflow Generator

Marcamos la opción YES, e introducimos el puerto por el cual el servidor va a escuchar todos los reportes generados y enviados por el SensorDMZ, en este caso, el puerto 12001.

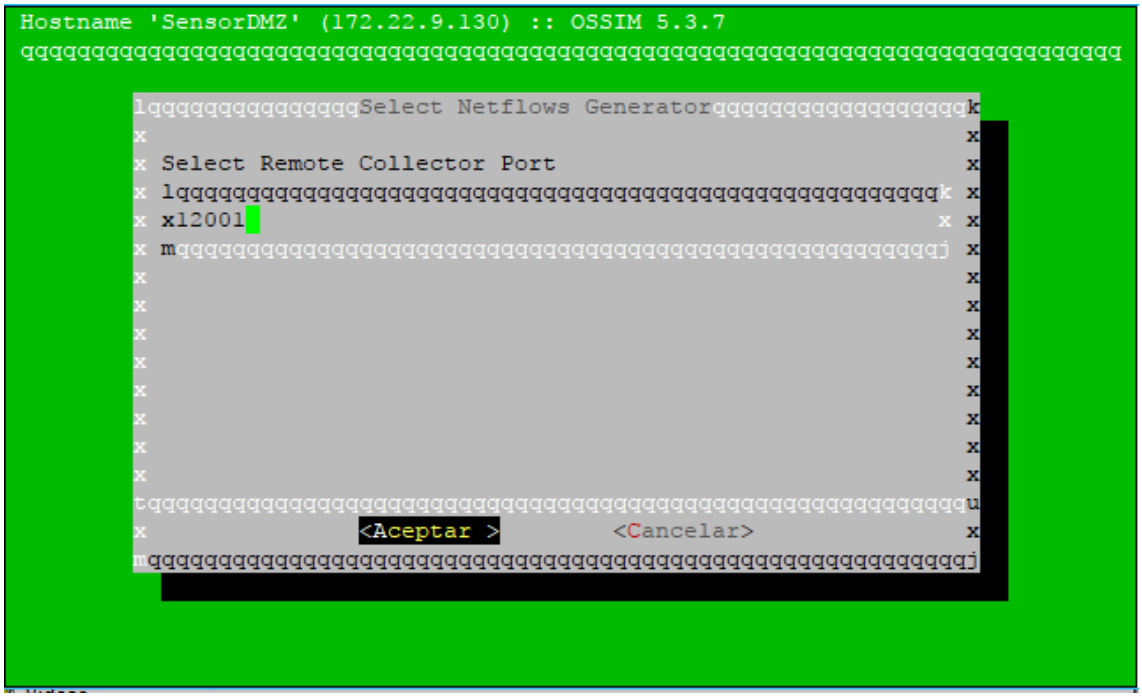


Figura 72 Configuración de envío de estadísticas de red en el SensorDMZ

Una vez que hemos configurado el sensor para que genere y envíe reportes periódicos de estadísticas de la red monitorizada al servidor OSSIM, debemos configurar dicho servidor para que escuche en el puerto 12001 y recolecte todos esos reportes.

Para ello, accedemos a

Configuration > Deployment > Sensor

Ahora debemos entrar en la página de configuración del SensorDMZ y desplazarnos a la zona inferior, concretamente a la sección

Netflow Collection Configuration

En dicha sección debemos introducir el puerto por el cual el servidor va a escuchar los reportes generados por el SensorDMZ, en este caso el 12001. También debemos seleccionar el color que va a utilizar el servidor OSSIM para dibujar las gráficas de estadísticas de uso en la interfaz web.

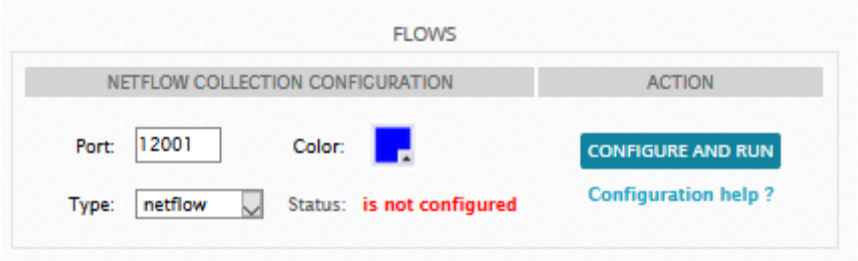


Figura 73 Configuración del servidor OSSIM para recolectar los reportes de estadísticas de red

Una vez realizada esta configuración, pulsamos el botón CONFIGURE AND RUN. Tras realizar esta configuración en todos los sensores desplegados en la red de la Diputación de Cádiz, debemos acceder a la sección

Environment > NetFlow

Figura 74 Sección de estadísticas de red en OSSIM

En esta sección podemos ver diferentes gráficas de uso de la red de la Diputación de Cádiz con diferentes colores, uno por cada uno de los sensores que genera reportes en el servidor OSSIM. Se pueden ver gráficas de tráfico TCP, UDP, ICMP u otros y aumentar y disminuir la escala de tiempo en días, semanas, meses y un año.

Más abajo, en esta misma sección, disponemos de la herramienta de búsqueda de estadísticas de sesiones y estadísticas de red de activos determinados.

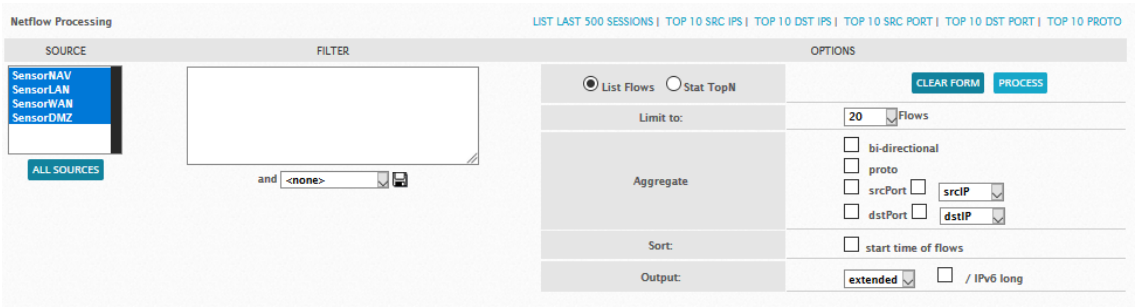
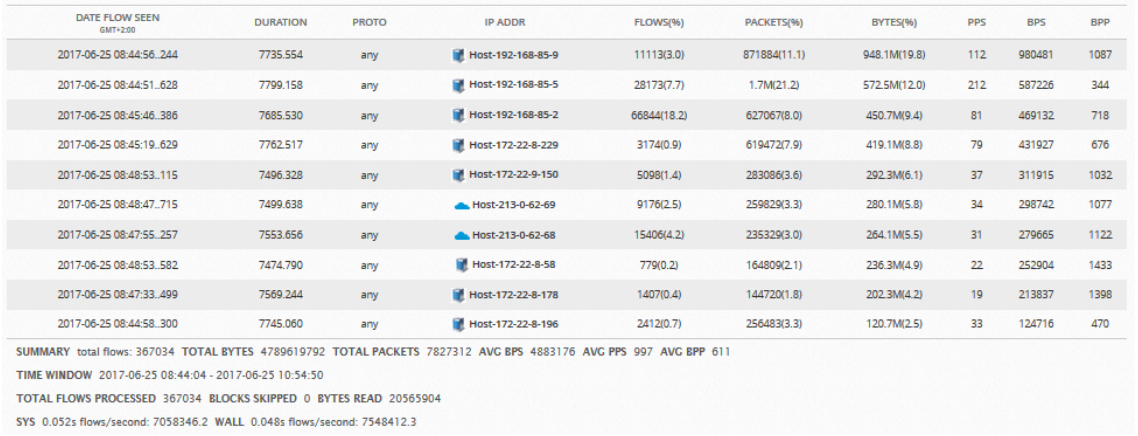


Figura 75 Sección de filtrado de datos estadísticos de la red de la Diputación de Cádiz

En esta sección se puede buscar en todos los reportes o en los generados por algunos sensores concretos, buscar activos concretos o modificar el modo de representación de la información de los datos estadísticos. Todas las búsquedas y filtrados que se realicen, se procesan dentro del espacio de tiempo introducido en la parte superior de la interfaz mediante las dos barras verticales desplazables.

Por ejemplo, se pueden mostrar las últimas 500 sesiones registradas en un determinado espacio de tiempo, las direcciones IPs de origen que más aparecen en la red, o los 10 protocolos más utilizados en la red.



DATE FLOW SEEN GMT+2:00	DURATION	PROTO	IP ADDR	FLOWS(%)	PACKETS(%)	BYTES(%)	PPS	BPS	BPP
2017-06-25 08:44:56..244	7735.554	any	Host-192-168-85-9	11113(3.0)	871884(11.1)	948.1M(19.8)	112	980481	1087
2017-06-25 08:44:51..628	7799.158	any	Host-192-168-85-5	28173(7.7)	1.7M(21.2)	572.5M(12.0)	212	587226	344
2017-06-25 08:45:46..386	7685.530	any	Host-192-168-85-2	66844(18.2)	627067(8.0)	450.7M(9.4)	81	469132	718
2017-06-25 08:45:19..629	7762.517	any	Host-172-22-8-229	3174(0.9)	619472(7.9)	419.1M(8.8)	79	431927	676
2017-06-25 08:48:53..115	7496.328	any	Host-172-22-9-150	5098(1.4)	283086(3.6)	292.3M(6.1)	37	311915	1032
2017-06-25 08:48:47..715	7499.638	any	Host-213-0-62-69	9176(2.5)	259829(3.3)	280.1M(5.8)	34	298742	1077
2017-06-25 08:47:55..257	7553.656	any	Host-213-0-62-68	15406(4.2)	235329(3.0)	264.1M(5.5)	31	279665	1122
2017-06-25 08:48:53..582	7474.790	any	Host-172-22-8-58	779(0.2)	164809(2.1)	236.3M(4.9)	22	252904	1433
2017-06-25 08:47:33..499	7569.244	any	Host-172-22-8-178	1407(0.4)	144720(1.8)	202.3M(4.2)	19	213837	1398
2017-06-25 08:44:58..300	7745.060	any	Host-172-22-8-196	2412(0.7)	256483(3.3)	120.7M(2.5)	33	124716	470

SUMMARY total flows: 367034 TOTAL BYTES 4789619792 TOTAL PACKETS 7827312 AVG BPS 4883176 AVG PPS 997 AVG BPP 611
TIME WINDOW 2017-06-25 08:44:04 - 2017-06-25 10:54:50
TOTAL FLOWS PROCESSED 367034 BLOCKS SKIPPED 0 BYTES READ 20565904
SYS 0.052s flows/second: 7058346.2 WALL 0.048s flows/second: 7548412.3

Figura 76 Información estadística de la red de la Diputación de Cádiz

9.5.4 Niveles de importancia de activos

Tras la entrevista con EPICSA para la realización de este proyecto, se estableció el requisito R-05, consistente en que el sistema SIEM debe ofrecer la posibilidad de establecer niveles de importancia en los activos.

OSSIM ofrece la posibilidad de establecer niveles de importancia en activos para que, dicho nivel de importancia, tenga influencia a la hora de determinar el riesgo real de un evento de seguridad generado en algún componente de OSSIM relacionado con esos activos. Este nivel de importancia también se puede definir como el nivel de riesgo de un activo de sufrir un ataque informático.

Para los activos de la red de la Diputación de Cádiz, se establece el siguiente baremo de importancia desde 1 a 5, siendo 1 el menos importante y 5 el más importante.

Nivel	Activos involucrados
1	-
2	Equipos personales
3	-
4	Servidores
5	Componentes OSSIM DMZ Servidores con conexión a DMZ

Tabla 19 Nivel de importancia de activos

Se establece un nivel de importancia 2 (medio-bajo) para todos los equipos personales conectados a la red de la Diputación de Cádiz ya que, al estar en la red local, están protegidos por todos los cortafuegos desplegados y no es muy probable que sufran un ataque.

Se establece un nivel importancia 4 (medio-alto) para todos los servidores desplegados en la red de servidores de la Diputación de Cádiz ya que, en esta red, están desplegados servidores importantes como controladores de dominio, servidores DNS, servidores de almacenamiento, servidores de máquinas virtuales, etc.

Se establece un nivel importancia 5 (alto) para todos los componentes OSSIM (servidor y sensores), ya que son el núcleo principal del sistema SIEM. También se establece este nivel

para los servidores desplegados en la DMZ, ya que son servidores que ofrecen servicios públicos, por lo que son de acceso público y es probable que puedan recibir ataques informáticos. También se establece este nivel de importancia para los servidores que conectan directamente con la DMZ, ya que, algunos servidores de la DMZ obtienen recursos de servidores internos.

En OSSIM, para establecer el nivel de importancia de un activo, debemos introducirlo en su página de edición en

Deployment > Assets & Groups

Buscamos el activo al que queremos cambiar el nivel de importancia y seleccionamos el botón de edición, para acceder a su página de edición de características. Para seleccionar la importancia del activo, escogemos el valor deseado en el desplegable correspondiente

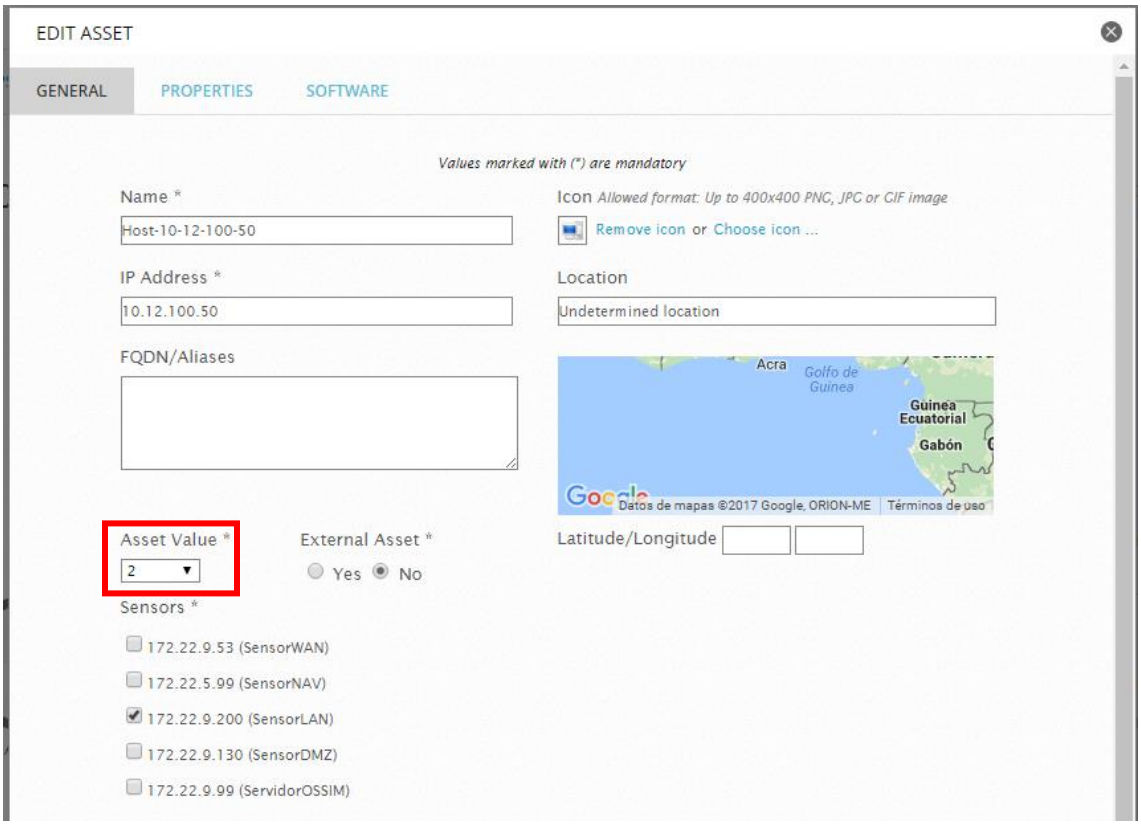


Figura 77 Configuración de nivel de importancia de un activo

Tras realizar toda esta configuración en todos los activos de la red de la Diputación de Cádiz, habremos cumplido con el requisito R-05 para la realización de este proyecto.

9.5.5 Gestión de usuarios

Tras la entrevista con EPICSA para la realización de este proyecto, se estableció el requisito R-06, consistente en que el sistema OSSIM debe ofrecer la posibilidad de conexión concurrente de usuarios administradores, en este caso y, como mínimo, dos usuarios.

El sistema OSSIM, aparte de ofrecer la posibilidad de simultaneidad en el uso del sistema por parte de varios usuarios, también ofrece un sistema de gestión de usuarios propio. Dicho sistema ofrece la posibilidad de crear, modificar y eliminar usuarios, así como limitar

qué partes del sistema OSSIM pueden administrar y filtrar la información de seguridad que pueden ver. Por ejemplo, podríamos tener un usuario por sede en la Diputación de Cádiz y configurar el sistema OSSIM de tal manera que cada usuario sólo pueda gestionar la información de seguridad de equipos de su sede correspondiente.

En este caso y, según lo establecido en la entrevista con EPICSA para la realización de este proyecto, deben existir dos usuarios administradores con control y visualización de todos los componentes OSSIM y de toda la información de seguridad generada en el sistema.

Para gestionar los usuarios en el sistema OSSIM, se debe acceder a través de la interfaz web a

Configuration > Administration > Users

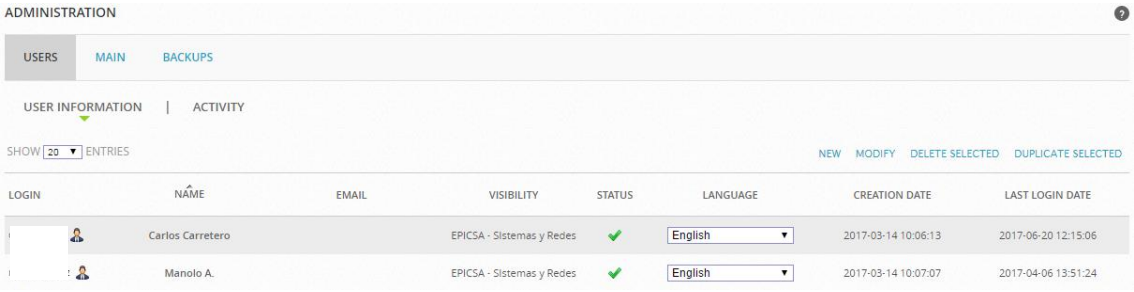


Figura 78 Sección de gestión de usuarios

Nota: Se han omitido los nombres de usuarios por motivos de confidencialidad.

A la hora de añadir un usuario podemos introducir sus datos personales, cambiar el idioma del sistema para ese usuario en concreto, obligar al usuario a cambiar su contraseña en su primer registro y editar los menús permitidos y la visualización de activos que dicho usuario va a tener.

Para añadir un usuario administrador, tal y como se establece en la especificación de requisitos de este proyecto, debemos seleccionar la opción *MAKE THIS USER A GLOBAL ADMIN* y dejar por defecto el valor de *Allowed Menus* y *Asset Filter* para que el usuario pueda acceder a todos los componentes de OSSIM y pueda visualizar toda la información de seguridad relacionada con todos los activos de la red de la Diputación de Cádiz.

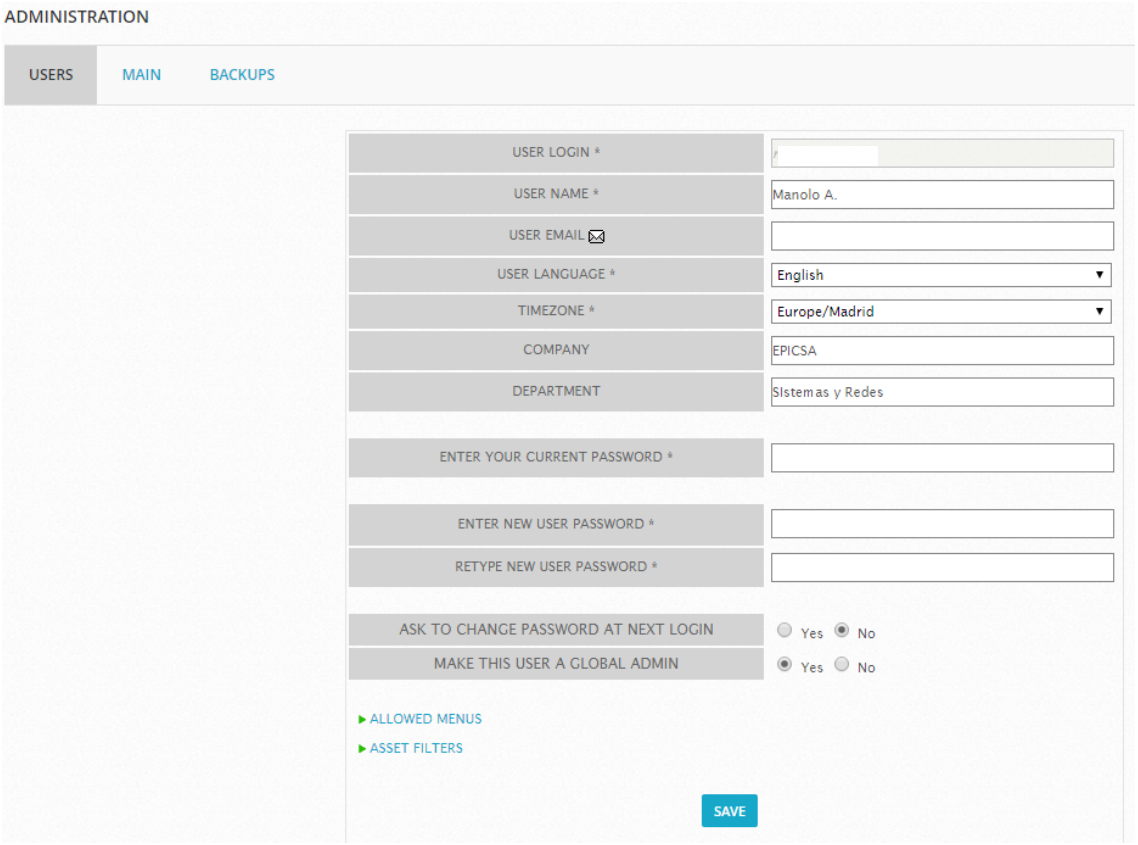


Figura 79 Creación de usuario administrador

Nota: Se ha omitido el nombre del usuario por motivos de confidencialidad.

9.5.6 Copias de seguridad

Tras la entrevista con EPICSA para la realización de este proyecto, se estableció el requisito R-08, consistente en que el sistema OSSIM debe ofrecer la posibilidad de realizar copias de seguridad de toda la información de seguridad recogida en la red de la Diputación de Cádiz.

El sistema OSSIM ofrece la posibilidad de realizar copias de seguridad de los eventos e información de seguridad recogidos por sus componentes y de toda la configuración realizada en el SIEM. Estas dos copias de seguridad se guardan como copias de seguridad separadas en el disco duro del sistema.

Para el cumplimiento de los requisitos establecidos tras la entrevista con EPICSA para la realización de este proyecto, se configurarán las copias de seguridad de eventos para que se realicen una vez al día a las 1 AM, para no influir en el trabajo en horario laboral. Se mantendrán las copias de seguridad en el sistema con antigüedad máxima de cinco días y serán encriptadas con una contraseña. Las copias de seguridad de la configuración de OSSIM tendrán la misma configuración, con diferencia de que, estas copias de seguridad, se realizarán a las 7 AM cada día.

La configuración de las copias de seguridad se realiza en

Configuration > Deployment > Main > Backup

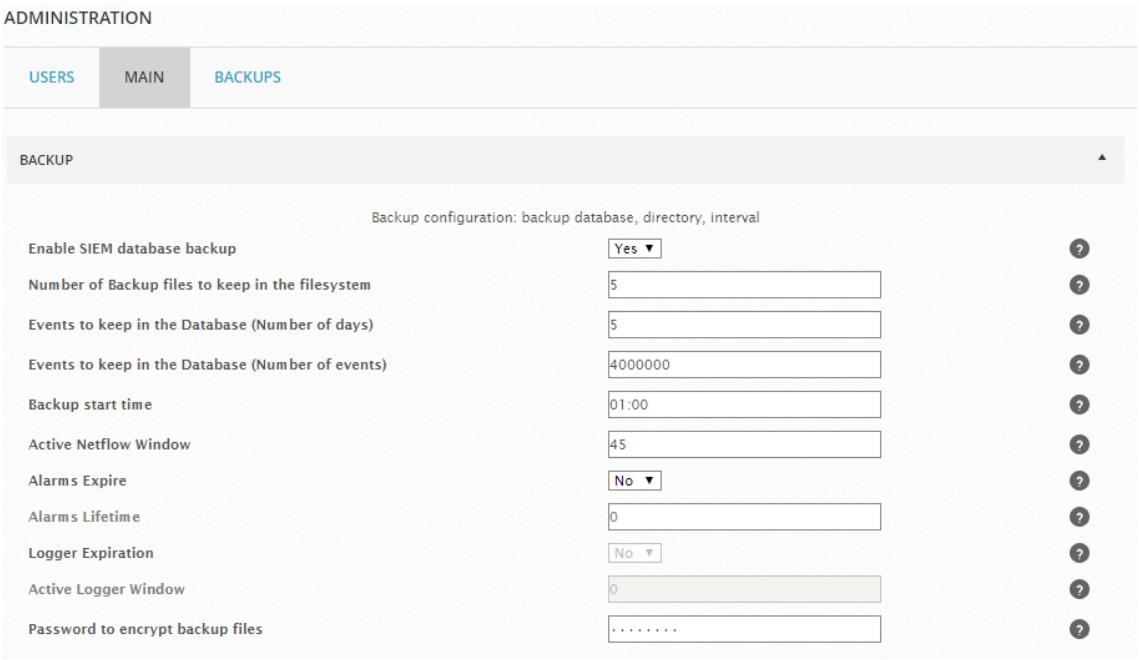


Figura 80 Sección de configuración de copias de seguridad

Toda la información relacionada con las copias de seguridad como aquellas ya realizadas, registros de errores, etc., se encuentra en

Configuration > Deployment > Bakcup

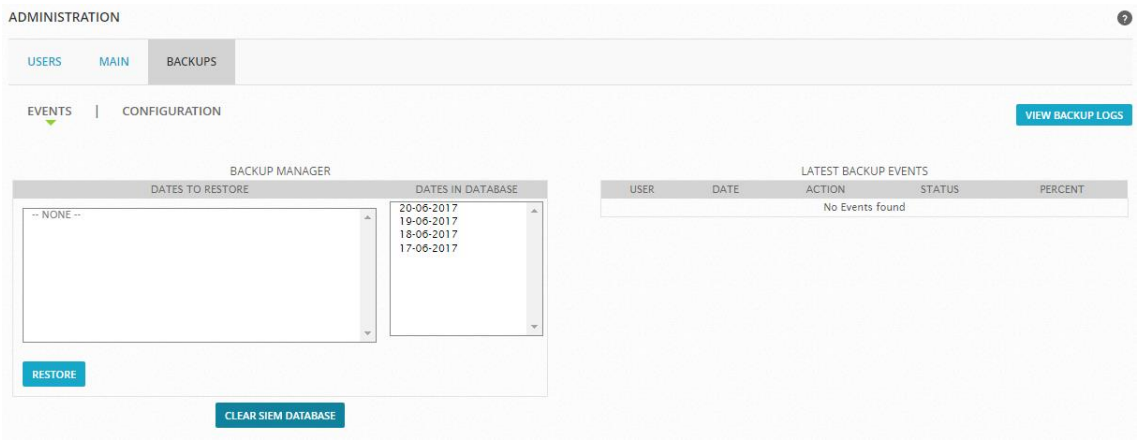


Figura 81 Sección de copias de seguridad de base de datos de eventos

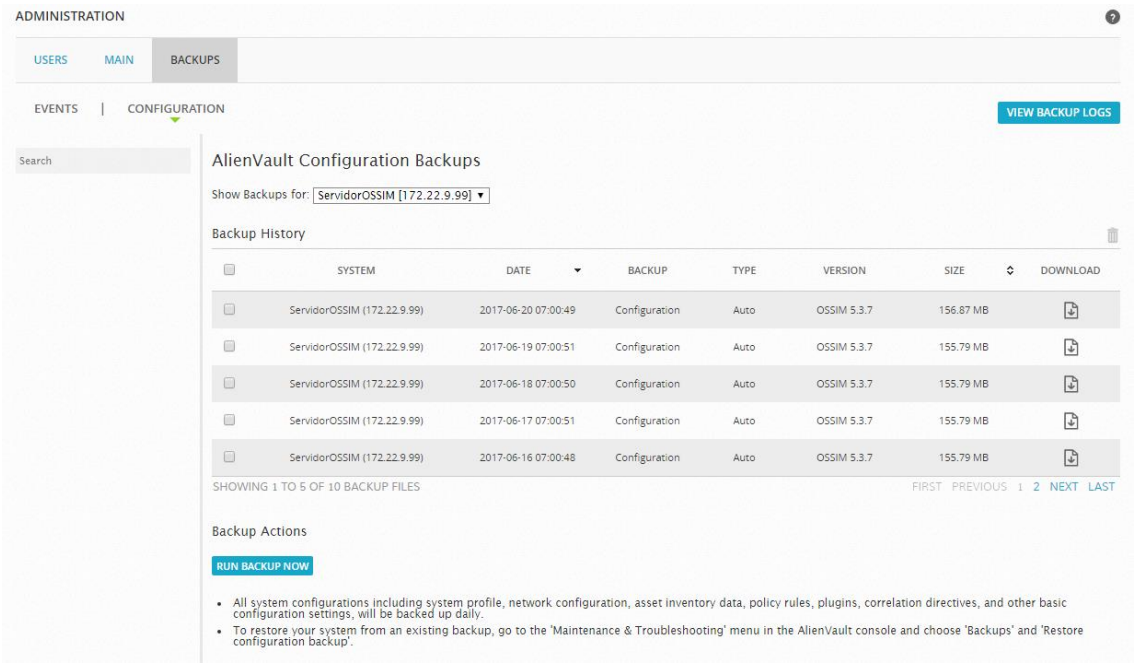


Figura 82 Sección de copias de seguridad de configuración

Si se desea restaurar el sistema OSSIM desde una copia de seguridad, ya sean la información de seguridad o la configuración, debemos realizar dicha acción desde la misma sección.

9.5.7 Motor de correlación

El motor de correlación del sistema OSSIM analiza todos los eventos de seguridad generados en el sistema para detectar riesgos de seguridad relacionados con patrones de comportamiento que involucren varios eventos de seguridad diferentes, varios activos diferentes, etc., transformando los datos en información mucho más útil.

Una vez que los eventos llegan al servidor después de ser normalizados en un sensor y después de que el servidor aplique las políticas correspondientes y le asigne valores de riesgo y prioridad al evento, el servidor aplica las directivas de correlación. Las directivas de correlación pueden generar eventos nuevos con nuevos valores de riesgo y prioridad que vuelven a pasar por el mismo proceso anterior.

Las directivas de correlación deciden si conectar eventos o no dependiendo de las reglas de correlación que contengan en su interior. En el sistema OSSIM, las directivas de correlación se encuentran en

Configuration > Threat Intelligence > Directives

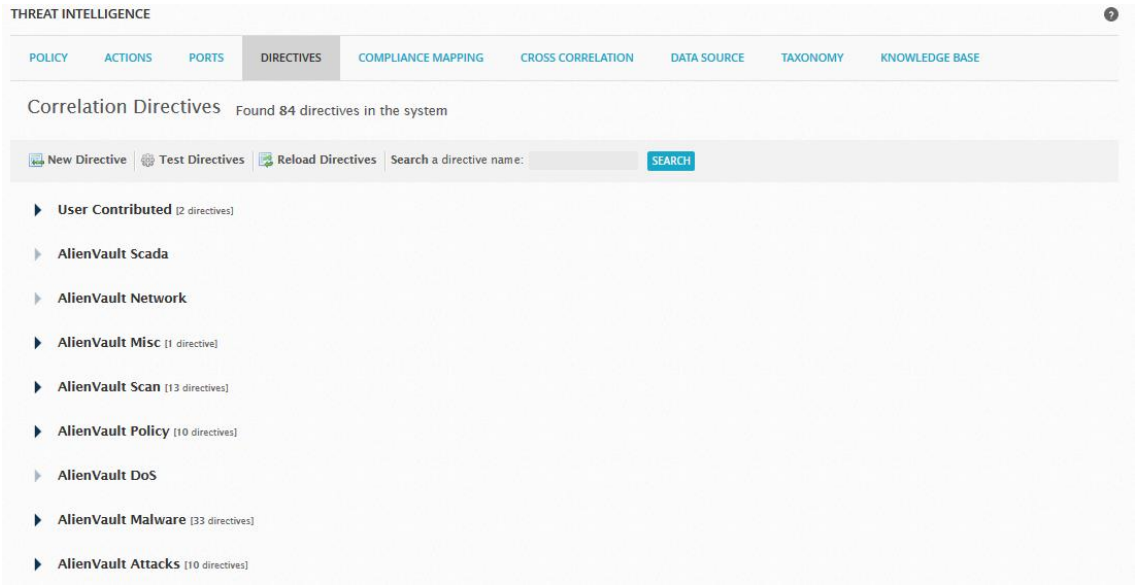


Figura 83 Sección de directivas de correlación en OSSIM

En la versión gratuita del SIEM de AlienVault, que es OSSIM, se incluyen unas pocas directivas de correlación ya configuradas.

Para ver un ejemplo del uso del motor de correlación se va a exponer un caso real ocurrido en la red de la Diputación de Cádiz. Se detectaron en la red de la Diputación de Cádiz un gran número de ataques de fuerza bruta a servidores de la red DMZ que tenían activo el servicio FTP, superando los 3000 ataques.

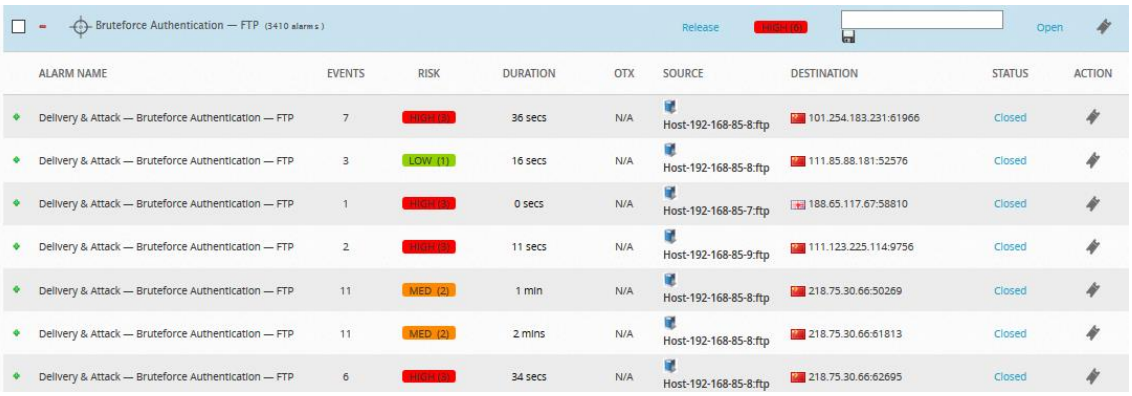


Figura 84 Ataques de fuerza bruta a la red DMZ de EPICSA

El gran número de alarmas por ataques de fuerza bruta llevó a la conclusión de que era necesario un mecanismo de análisis que alertara de cuando un ataque de fuerza bruta tuviera éxito, para así poder descartar todas las alarmas anteriores como ataques exitosos. Ese mecanismo de análisis lo ofrece OSSIM a través del motor de correlación. Para poder solucionar este problema, el motor de correlación debe poder relacionar los eventos de ataques de fuerza bruta con un evento que refleje un inicio de sesión externo de la misma dirección IP origen del ataque.

Primero, debemos crear la regla de Suricata (NIDS de OSSIM) que sea capaz de detectar un inicio de sesión exitoso en un servicio FTP.

```
alert tcp $HOME_NET 21 -> any any
(msg:"FTP External Login Successful"; content:"230 ";
pcre:"/230(\s+|-)(User|Logged|Welcome|In|Usuario|Conectado)/smi";
threshold: type limit, track by_dst, count 1, seconds 5;
classtype:successful-user; sid:4000006; rev:1;)
```

Figura 85 Regla de NIDS para detectar inicio de sesión en servicio FTP

Una vez que tenemos todos los elementos necesarios para crear la directiva de correlación, debemos idear la estructura de funcionamiento de la misma.

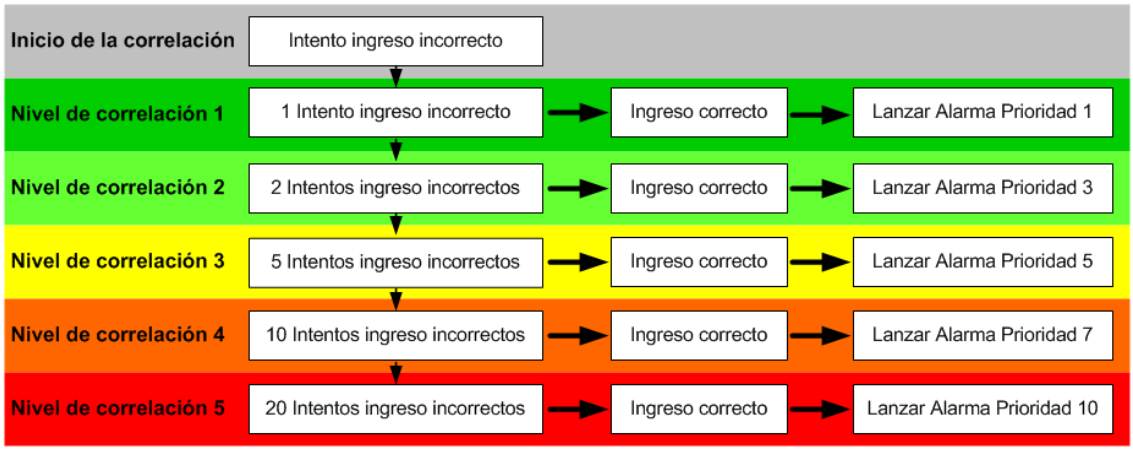


Figura 86 Estructura de directiva de correlación para ataques de fuerza bruta a servicios FTP exitosos

El modo de navegar dicha estructura de la directiva de correlación es el siguiente. Una vez que se detecta el evento de intento de ingreso fallido en el servicio FTP de un determinado activo de la red de la Diputación de Cádiz se inicia el procesamiento de la directiva de correlación en el nivel más bajo de riesgo, el nivel 1. Situándose el motor de correlación de OSSIM en dicho nivel, si en un determinado tiempo el sistema OSSIM detecta un ingreso correcto en el servicio FTP del mismo activo, OSSIM lanzará una alarma con un determinado valor de prioridad. Si el ingreso correcto no se produce, el sistema OSSIM esperará un determinado tiempo a que se produzcan más intentos fallidos de ingreso para incrementar el nivel de riesgo de la directiva de correlación. Si no se diera el caso de que se detectaran más intentos fallidos de ingreso en el servicio FTP del activo, se aborta el lanzamiento de la alarma. El procesamiento de la directiva de correlación es idéntico en cada nivel de riesgo, solo que cambian los valores de límites de tiempo, número de intentos fallidos de ingreso y nivel de prioridad de la posible alarma lanzada.

Una vez que hemos creado la estructura de funcionamiento de la directiva de correlación, debemos configurar dicha directiva en el sistema OSSIM. Para crear la directiva de correlación, debemos acceder a la sección de correlación y crear una nueva directiva. Las directivas de correlación creadas por el usuario aparecen en la sección USER CONTRIBUTED

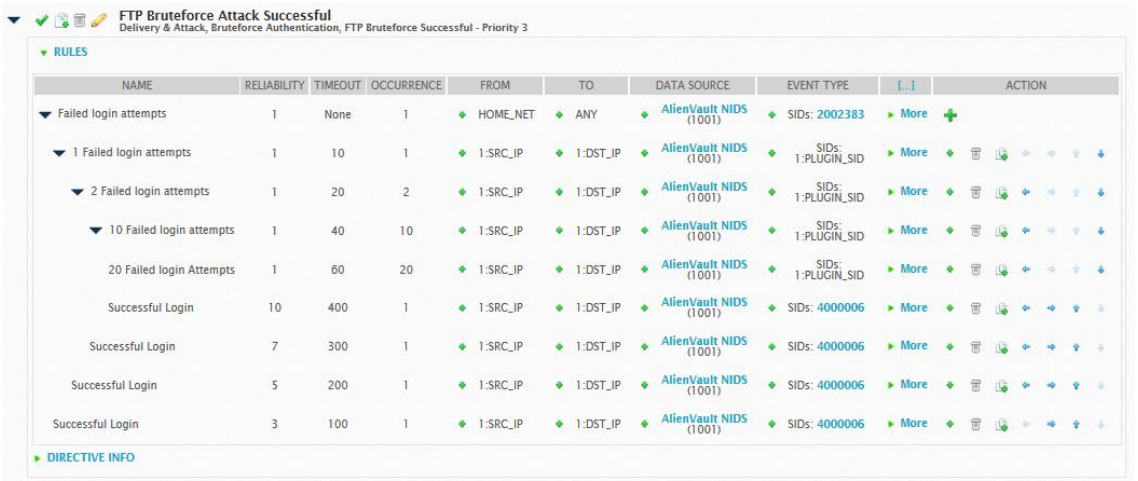


Figura 87 Directiva de correlación para ataques de fuerza bruta a servicios FTP exitosos

9.5.8 Correlación cruzada

La correlación cruzada es un tipo especial de correlación realizado por el sistema OSSIM que relaciona eventos de seguridad en red con vulnerabilidades detectadas en los equipos relacionados con dichos eventos de seguridad. Si se ha detectado un intento de explotación de una vulnerabilidad contra un activo de la empresa que, en principio, no tiene riesgo pero que, previamente, se le detectó esa vulnerabilidad, automáticamente el evento de seguridad se convierte en un evento de máximo riesgo.

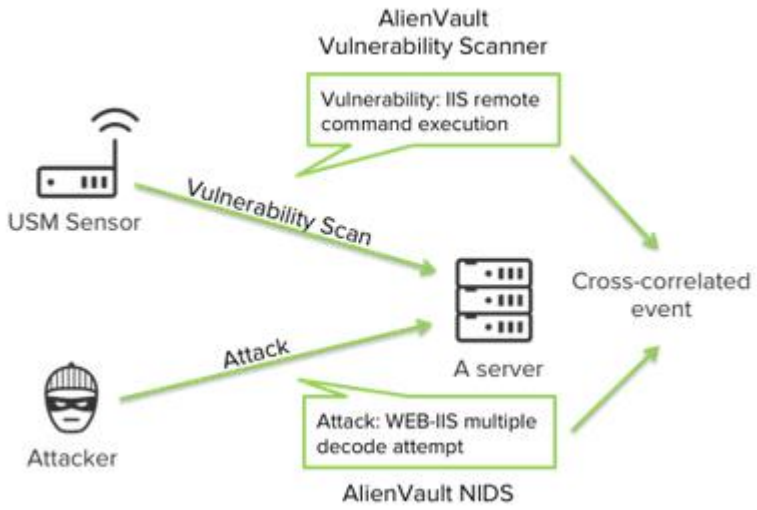


Figura 88 Correlación cruzada en OSSIM

En la instalación de OSSIM por defecto, se incluyen muchas directivas de correlación cruzada por defecto. Estas directivas de correlación se encuentran en el sistema OSSIM en

Configuration > Threat Intelligence > Cross Correlation

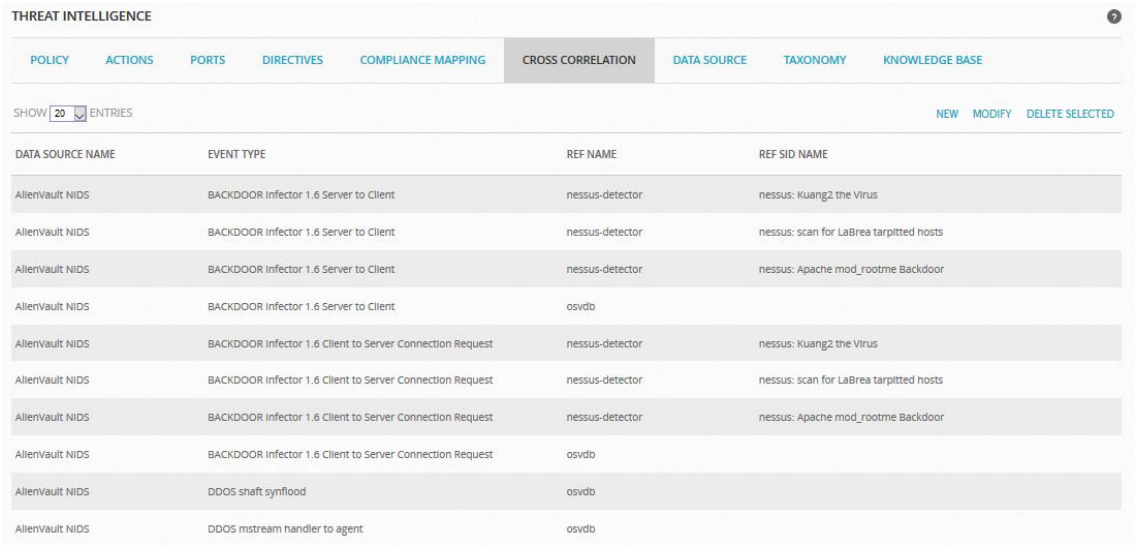


Figura 89 Sección de correlación cruzada en OSSIM

Por ejemplo, en la red de la Diputación de Cádiz se detectó un intento de explotación de una vulnerabilidad relacionada con la ejecución remota de comandos en el bash de una máquina con sistema operativo basado en Linux de la red DMZ de EPICSA, concretamente, la vulnerabilidad CVE-2014-6271.

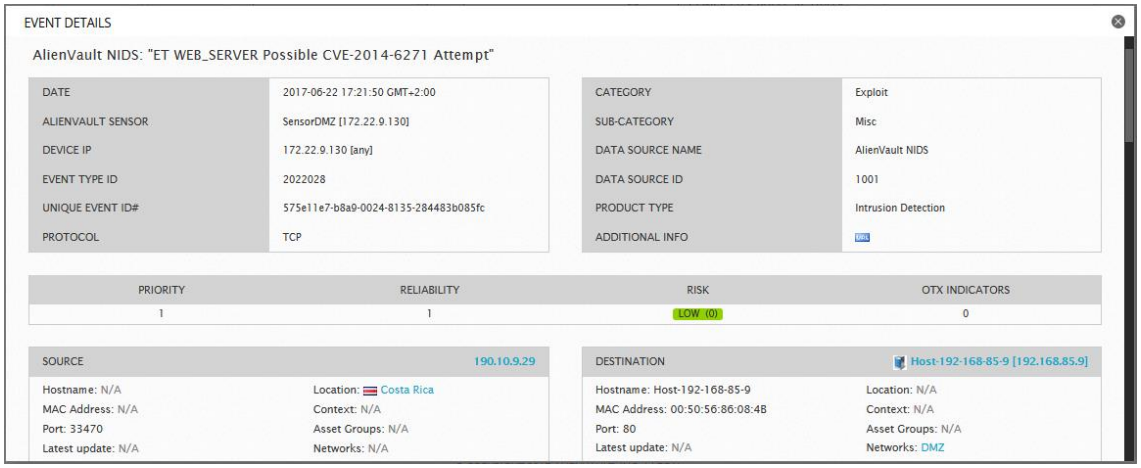


Figura 90 Intento de explotación de la vulnerabilidad CVE-2014-6271

Revisando los resultados de los análisis de vulnerabilidades periódicos realizados a ese activo concreto de la red DMZ de EPICSA, se detectó la existencia en dicho activo de la vulnerabilidad CVE-2014-6271.

Figura 91 Vulnerabilidad CVE-2014-6271 detectada

Al no existir una directiva de correlación cruzada por defecto en el sistema OSSIM que relacione ese intento de explotación de la vulnerabilidad CVE-2014-6271 con la existencia de la vulnerabilidad en el activo objetivo del ataque, es necesario crear dicha directiva.

Para ello, pulsamos el botón New en la sección de correlación cruzada e introducimos la información necesaria.

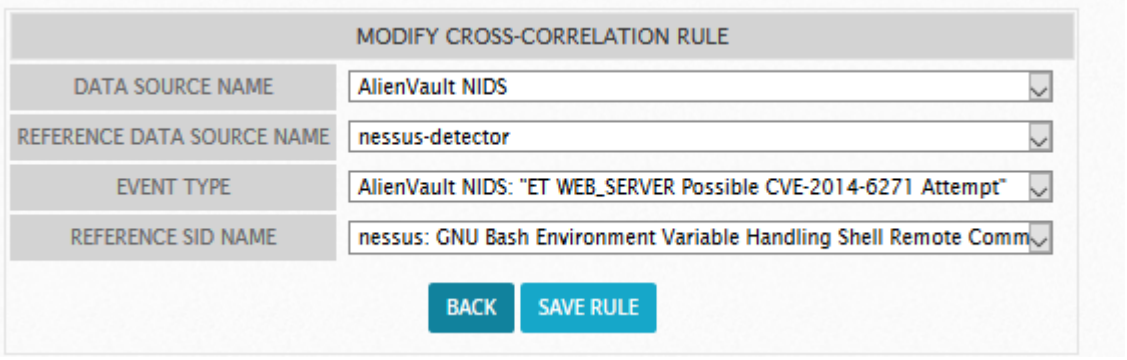


Figura 92 Configuración de directiva de correlación cruzada

Los campos DATA SOURCE NAME y EVENT TYPE se refieren al intento ataque que se puede en la red que OSSIM está monitorizando y los campos REFERENCE DATA SOURCE NAME y REFERENCE SID NAME se refieren a la vulnerabilidad presente en el activo objetivo del intento de ataque.

A continuación, se puede observar, que una vez que la correlación cruzada, cuando se detecta el intento de ataque y en el equipo con la vulnerabilidad, el evento aumenta su riesgo y prioridad y se convierte en una alarma.

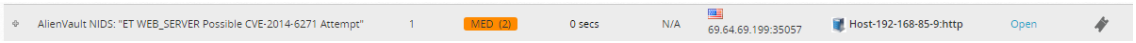


Figura 93 Alarma generada por directiva de correlación cruzada

9.5.9 Políticas del SIEM

Las políticas en el sistema OSSIM son un componente muy importante a la hora del funcionamiento diario de OSSIM. Las políticas nos permiten acciones como:

- Filtrar eventos de seguridad que generan falsos positivos.
- Modificar los valores de riesgo de los eventos de seguridad, por ejemplo, aumentar el riesgo de un evento de seguridad si aparece relacionado con una activo o grupo de activos en concreto.
- Enviar correos ante ciertos eventos o alarmas de seguridad.

Las políticas se componen de condiciones y consecuencias. Las condiciones determinan que eventos serán procesados por la política y las consecuencias determinan que acciones se deben tomar ante dichos eventos.

Toda la configuración y gestión de políticas en el sistema OSSIM se realiza en

Configuration > Threat Intelligence > Policy

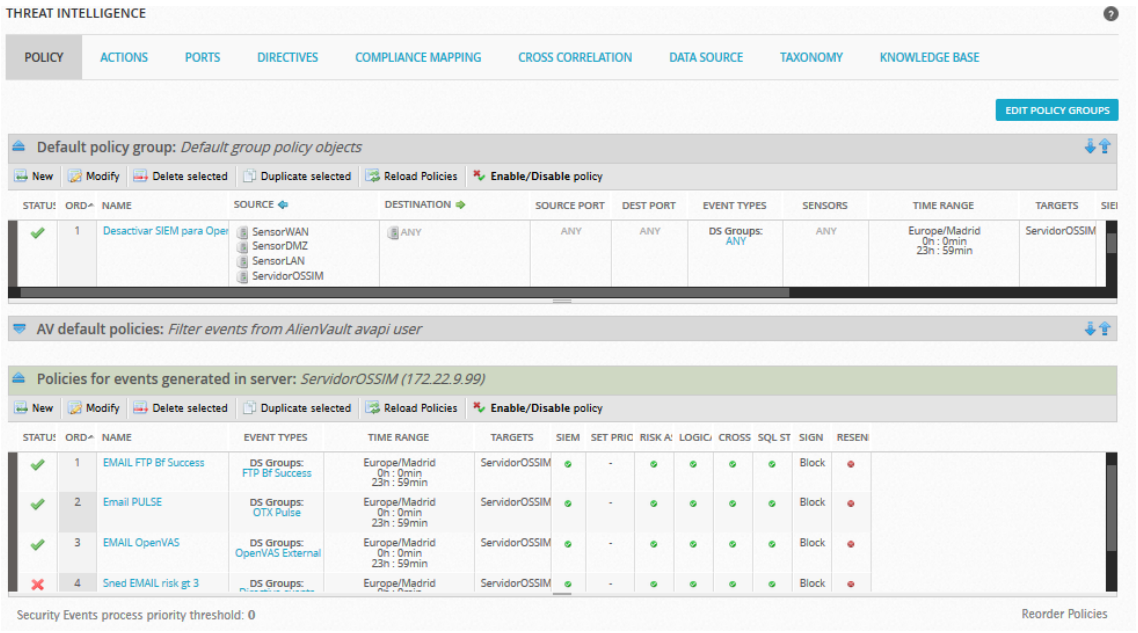


Figura 94 Sección de políticas en OSSIM

Por ejemplo, en el sistema OSSIM de la Diputación de Cádiz se ha configurado una política de seguridad que evita que los sensores generen eventos de seguridad sobre el tráfico que ellos mismos generan para los escáneres de vulnerabilidades. Dicha política elimina el almacenamiento de los eventos de seguridad que tengan como origen alguno de los sensores OSSIM desplegados en la red de la Diputación de Cádiz.

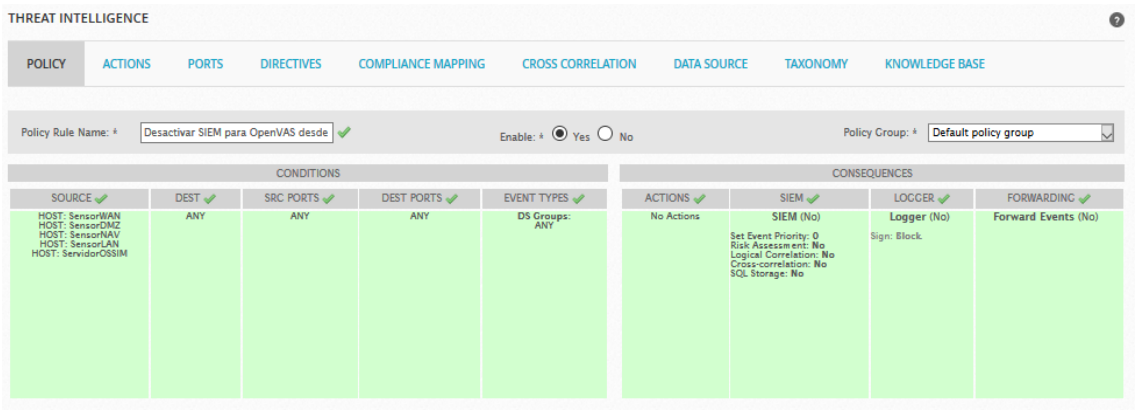


Figura 95 Política de filtrado de eventos de seguridad

También se han configurado políticas de seguridad que envían correos automáticamente cuando se detectan alarmas por ataques de fuerza bruta con inicio de sesión, por análisis de vulnerabilidades externos y por información relacionada con AlienVault OTX.

Se muestra la configuración de la política de envío de emails ante un ataque de fuerza bruta con inicio de sesión, siendo la configuración de las demás políticas idéntica.

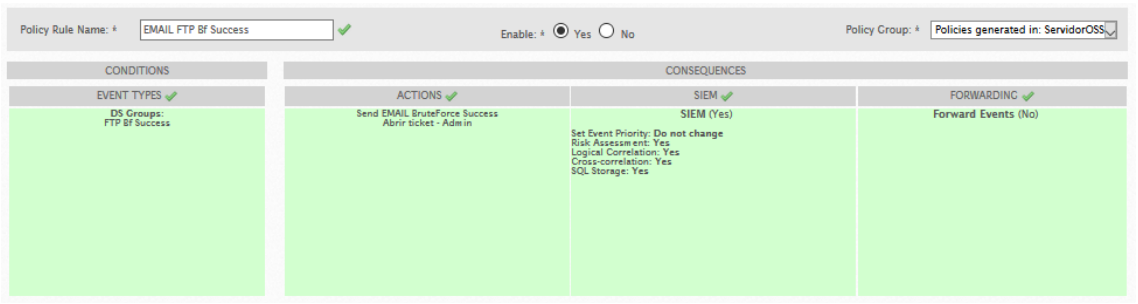


Figura 96 Política de acciones ante eventos de seguridad

En el sistema OSSIM, el envío de correos se configura en

Configuration > Threat Intelligence > Actions > New

Se muestra a continuación la configuración del email relacionado con los ataques de fuerza bruta, siendo la configuración de los otros emails idéntica, simplemente cambiando el contenido del mismo.

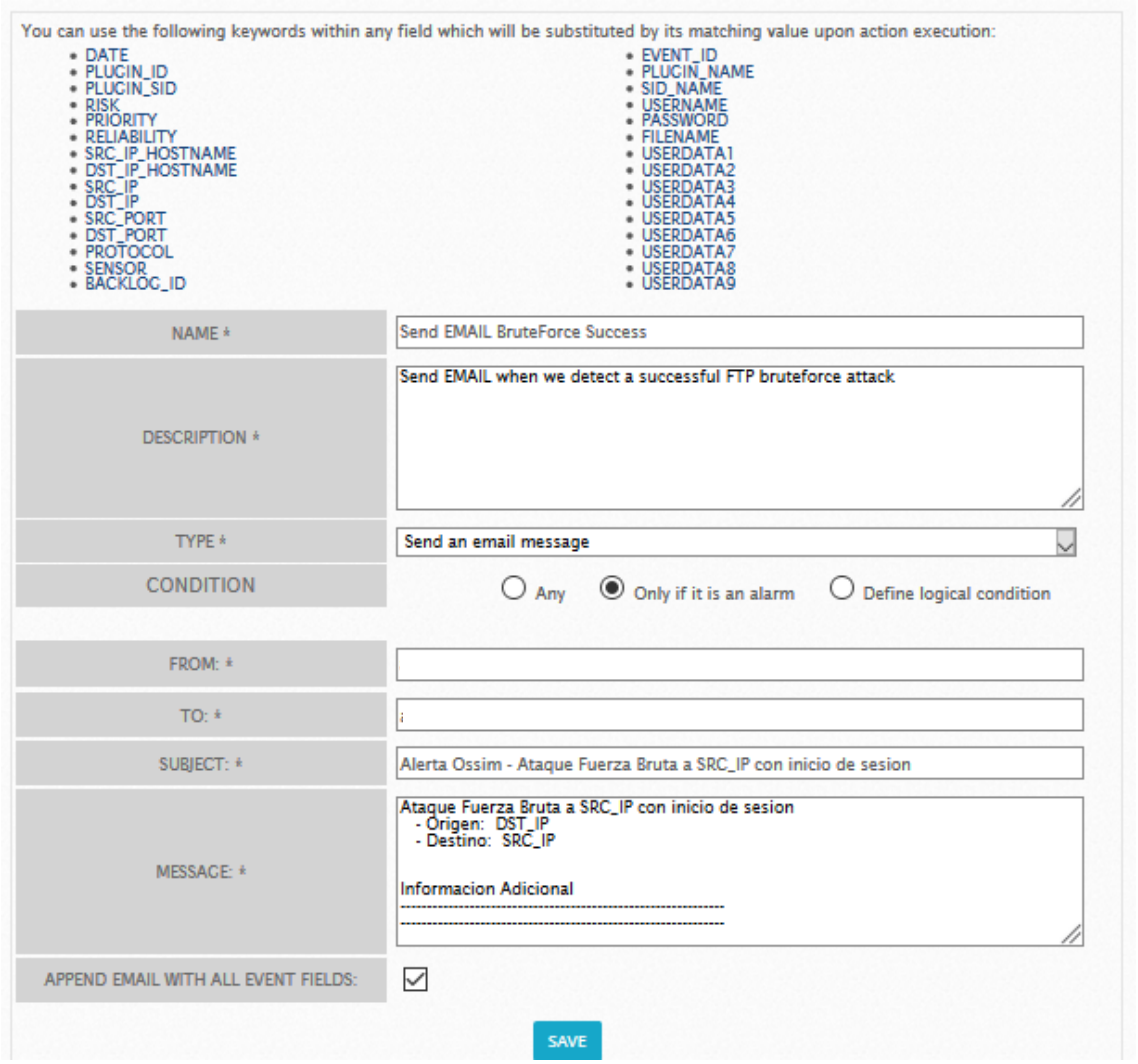


Figura 97 Email configurado para una política de seguridad

Nota: Se han omitido las direcciones de correo por motivos de confidencialidad.

Podemos ver que, ante la generación de la alarma, el correo es enviado al destinatario seleccionado.

Figura 98 Alarma de seguridad que genera un envío de email

Figura 99 Email generado ante evento de seguridad

9.5.10 Actualización automática

Debido a la alta frecuencia de aparición de nuevos patrones de ataques, vulnerabilidades y fallos de seguridad en software, sistemas operativos, hardware, etc., es necesario que el sistema OSSIM se mantenga actualizado diariamente, en lo referente a nuevas firmas para los IDS y el escáner de vulnerabilidades, así como en lo referente a las actualizaciones del propio software de OSSIM.

Aunque no se ha establecido como requisito inicial de este proyecto, se han configurado todos los componentes del sistema OSSIM para que se actualicen automáticamente todos los días. Para que dicha actualización no interfiera en el trabajo de mantenimiento y/o supervisión del sistema OSSIM, se ha configurado dicha actualización automática en horario no laboral, aunque se ha aproximado lo máximo posible para que, si surge un problema con la actualización, sea resuelta lo antes posible.

Para configurar las actualizaciones automáticas, entramos en un componente OSSIM mediante una sesión SHH, en este caso, con el servidor. Accedemos a la consola del servidor mediante la opción *Jailbreak System* y editamos el fichero *cron* emitiendo el comando *crontab –e* para añadir la configuración deseada.

```
# m h  dom mon dow   command

0 6  * * * /usr/bin/alienvault-update > /root/av_update.txt 2>&1
```

Figura 100 Actualización automática de componentes OSSIM

La actualización se realizará todos los días a las 6:00 AM y se guardará el resultado en un fichero de registro, por si fuera necesaria dicha información para tareas de depuración y/o solución de errores.

9.5.11 Conexión con AlienVault Open Threat Exchange

Como se ha especificado con anterioridad, el sistema OSSIM ofrece la posibilidad de conectarse con la comunidad de peligros emergentes AlienVault Open Threat Exchange (OTX) con todas las ventajas que eso conlleva: actualización diaria de peligros emergentes, suscripción automática a nuevos peligros, etc.

Para configurar el sistema OSSIM para que se conecte al sistema OSSIM debemos registrarnos en OTX en el enlace https://otx.alienvault.com/accounts/signup/. Una vez realizado el proceso de instalación, debemos introducir la clave generada en nuestro sistema OSSIM para enlazarlo a nuestra cuenta de OTX. Para ello, accedemos a

Configuration > Open Threat Exchange > Actions > Enter OTX Key

Introducimos la clave generada en el registro en OTX y aceptamos la configuración. Tras esto, nuestro sistema OSSIM estará conectado a OTX y se suscribirá automáticamente a todas las entradas con información creadas por AlienVault. La suscripción a entradas de usuarios diferentes debe ser manual.

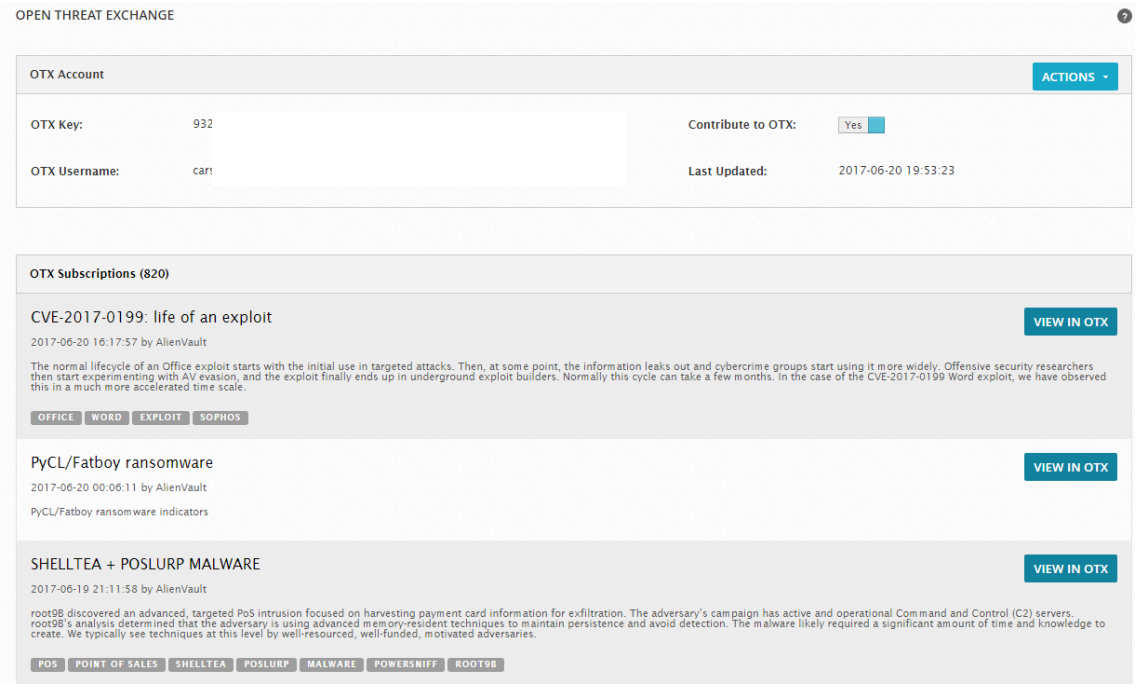


Figura 101 Sección de información de AlienVault OTX

Nota: Se ha omitido información de registro en OTX por motivos de confidencialidad.

A continuación, se puede ver un caso real ocurrido en la red de la Diputación de Cádiz, en la que la aparición de una dirección IP externa en la red, generó una alarma relacionada con un pulso de OTX.

Figura 102 Alarma generada por AlienVault OTX

9.5.12 Sistema de comunicación entre usuarios

El sistema OSSIM posee un sistema de comunicación entre usuarios para la respuesta ante eventos de seguridad al que denomina ticket. Un ticket en OSSIM sirve para controlar que eventos de seguridad ocurrieron y que acciones se tomaron ante tales eventos. Los tickets también sirven para asignar la investigación de eventos de seguridad a diferentes usuarios.

Los tickets se pueden generar automáticamente basándose en una política configurada, automáticamente al detectar una vulnerabilidad en un activo, manualmente durante la investigación de un evento de seguridad y manualmente para cualquier tipo de información no relacionada con eventos de seguridad.

En el sistema OSSIM, toda la información relacionada con los tickets se encuentra en

Analysis > Tickets

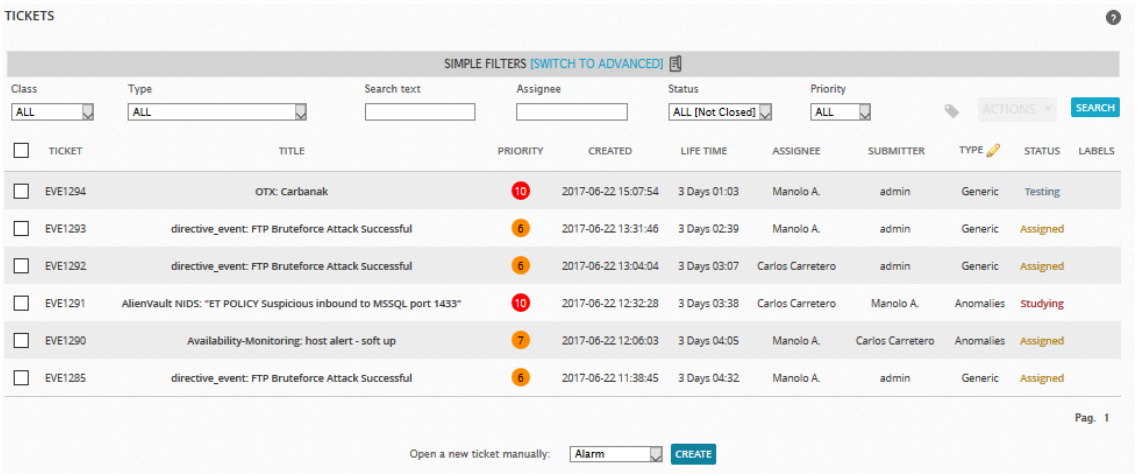


Figura 103 Sección de tickets en OSSIM

Si pulsamos en un ticket podemos ver la información específica del ticket, así como todo el histórico de cambios y acciones que se han tomado en relación al ticket. También disponemos de una sección inferior para cambiar el estado del ticket, asignárselo a otro usuario y realizar comentarios.

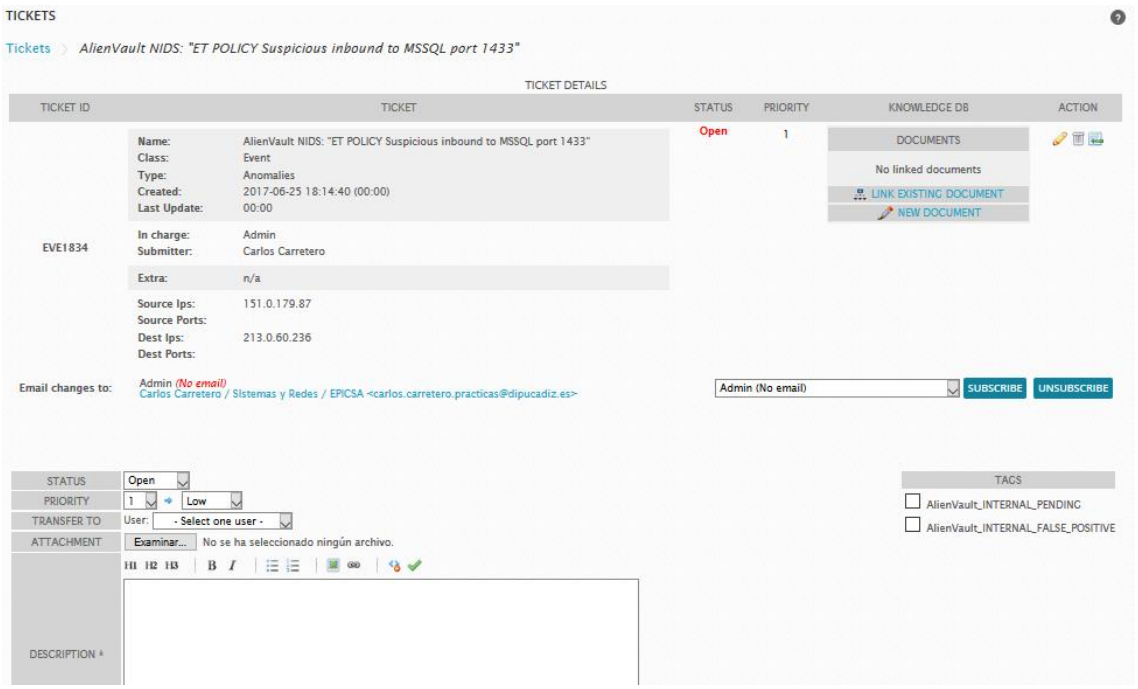


Figura 104 Información específica sobre un ticket

Automáticamente, el sistema OSSIM enviará emails a los usuarios suscritos al ticket informando de cualquier cambio y/o comentario que se haya realizado en el mismo.

Tal y como se han configurado políticas para el envío de emails personalizados ante las alarmas de ataque de fuerza bruta, de análisis de vulnerabilidades externo y de información relacionada con OTX, también se han configurado dichas políticas para que generen un ticket de esas alarmas automáticamente. Tras configurar la acción de generar un ticket automáticamente, debemos asignárselo a las políticas de envío de emails.

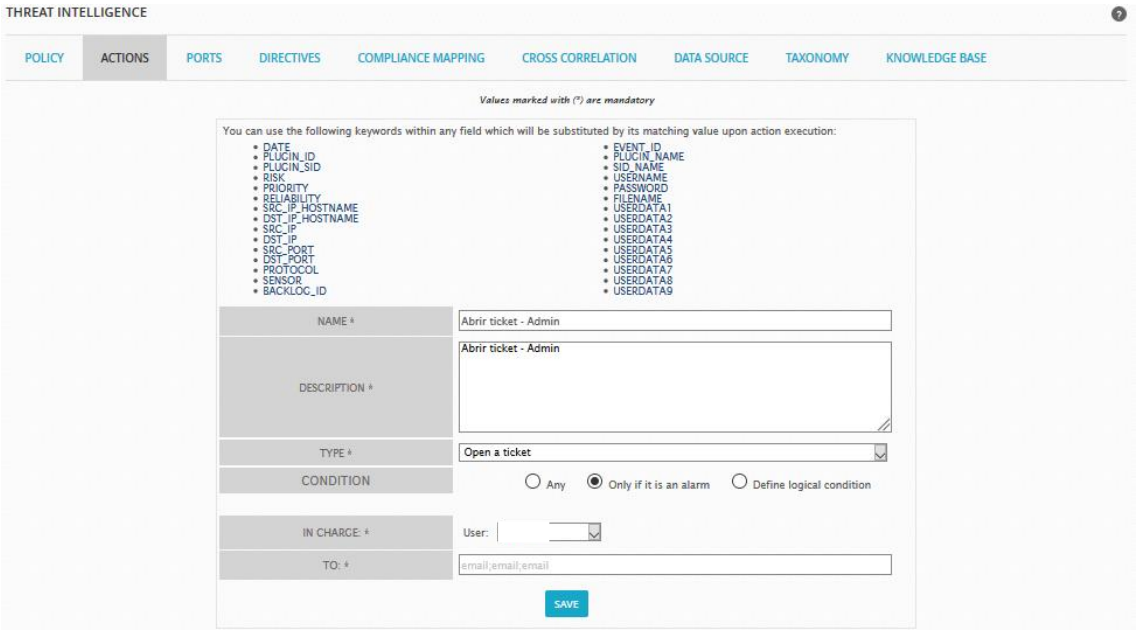


Figura 105 Acción de generar ticket

Nota: Se ha omitido el nombre del usuario por motivos de confidencialidad.

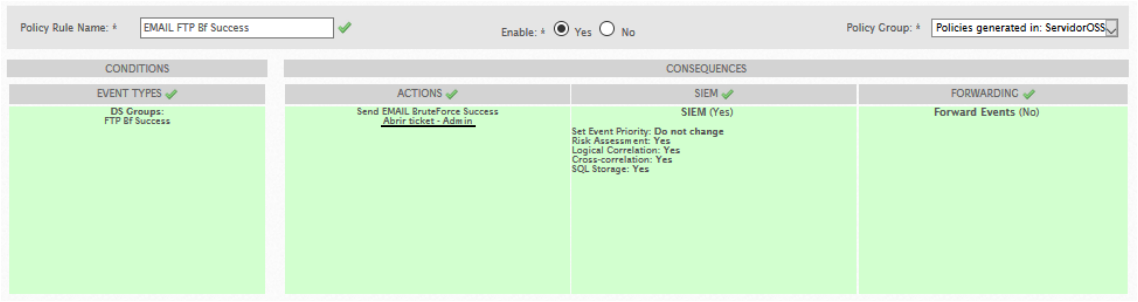


Figura 106 Política de seguridad con generación automática de ticket

10 Planificación temporal

La planificación de este proyecto se enmarca dentro de un periodo temporal de 4 meses, desde el 1 de Marzo de 2017 hasta el 1 de Julio de 2017.

El desglose de tareas a realizar ordenadas según su ejecución durante la realización del proyecto se detalla en la siguiente figura.

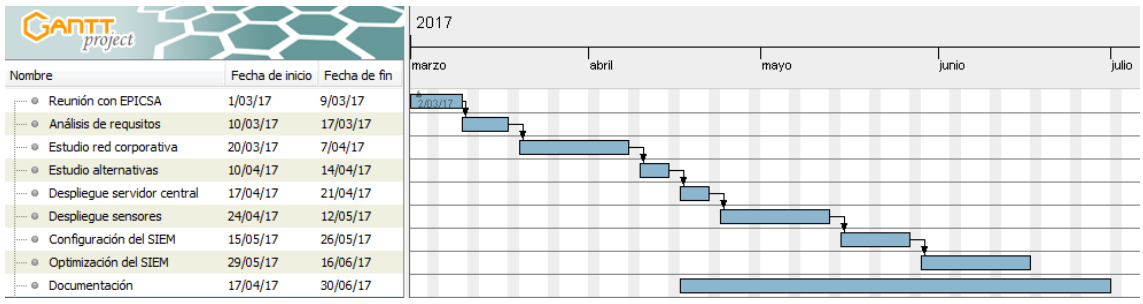


Figura 107 Planificación temporal

11 Resumen del Presupuesto

El resumen del presupuesto para el proyecto de implantación de un sistema de seguridad de información y administración de eventos en la red de la Diputación de Cádiz es el siguiente:

	Precio (€)
Cableado	20,88
Equipos	14.608,70
Personal	4.853,00
Software	0,00
Total	**19.482,58**

Tabla 20 Resumen del presupuesto

12 Orden de prioridad de los documentos

1. Especificaciones del sistema.
2. Mediciones.
3. Presupuesto.
4. Memoria.
5. Anexos
6. Estudio teórico.

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

REF: 0000001

ESTUDIO TEÓRICO

CLIENTE: EMPRESA PROVINCIAL DE INFORMACIÓN DE CÁDIZ S.A. (EPICSA)
PLAZA MADRID S/N, EDIFICIO CARRANZA, FONDO SUR, LOCAL 10, 11010 CÁDIZ
956261500

AUTOR: CARLOS CARRETERO AGUILAR
INGENIERO INFORMÁTICO
25603515-F
CARLOS.CARRETEROAGUILAR@ALUM.UCA.ES

FIRMADO:
SOLICITANTE AUTOR

CÁDIZ, A 1 DE JULIO DE 2017

1 Estructuración y modularización de redes

1.1 Diseño de la jerarquía de red

En la mayoría de diseños de redes que se realizan actualmente, ya sean redes LAN o redes WAN, se utiliza un modelo de modularización que aproxima la red a una estructura jerárquica bien definida. El modelo de red jerárquico ofrece una vista modular de la red, que permite diseñar y construir una red escalable. Este modelo divide la red en tres capas bien diferenciadas:

- **Capa de acceso.**
- **Capa de distribución.**
- **Capa de núcleo.**

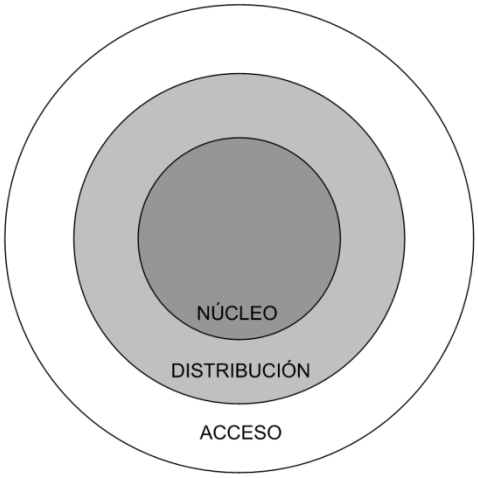


Figura 108 Diagrama básico de jerarquía de red en capas

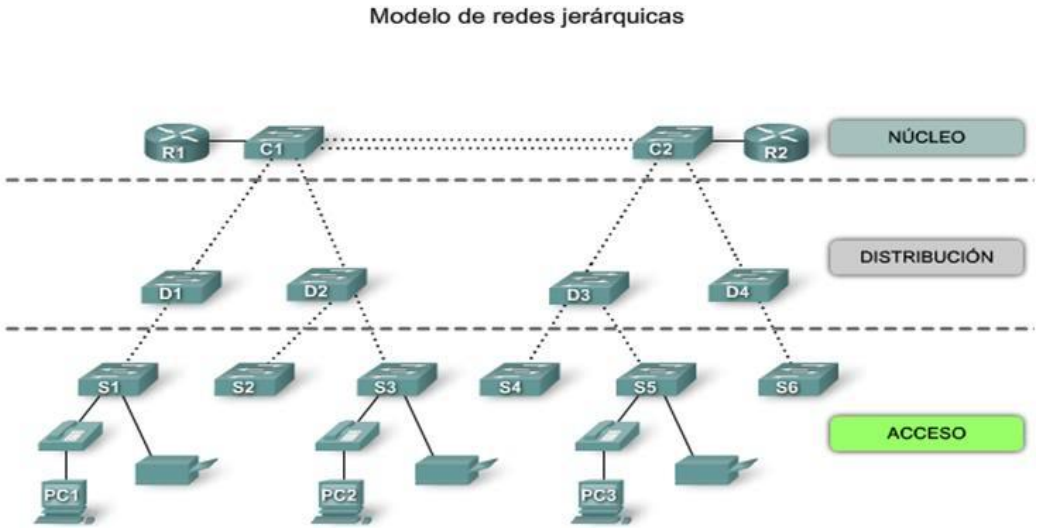


Figura 109 Topología básica de red con jerarquía de 3 capas

1.1.1 Capa de acceso

La capa de acceso es el primer nivel, o borde, de una red. En esta capa se sitúan todos los dispositivos finales, como ordenadores, cámaras, impresoras y todo aquel dispositivo que

necesitará de una red para el desarrollo de sus funcionalidades. En esta capa también se sitúan aquellos dispositivos que extienden el acceso a la red más allá de la capa de acceso, por ejemplo, los puntos de acceso que proveen de conexión inalámbrica. La capa de acceso debe asegurar el acceso a la red y proveer seguridad y calidad de servicio al acceso de los recursos de la red.

El acceso a la red, por parte de la capa de acceso, puede ser proporcionado mediante dos métodos principales:

- **Usando conmutadores de capa 2**. Los conmutadores de capa 2 de la capa de acceso contienen los puertos para usuarios finales y los puertos que conectan con la capa de distribución. Las VLANs pueden ser utilizadas para disminuir el tamaño de los dominios de broadcast de la red y para separar el tráfico de red. El transporte del tráfico entre conmutadores de capa de acceso y capa de distribución suele realizarse mediante enlaces troncales que siguen el protocolo IEEE 802.1Q. Un conmutador de capa 3 también puede proporcionar conexión entre VLANs diferentes.
- **Usando conmutadores de capa 3 (WAN).** El enrutamiento del acceso provee un punto de entrada para oficinas remotas, así como a Internet. Esto se consigue utilizando tecnologías WAN combinadas con características como propagación de rutas, filtrado de paquetes, autenticación, etc.

Los conmutadores situados en la capa de acceso deben estar conectados con enlaces redundantes a los conmutadores de la capa de distribución. Una buena práctica es configurar una VLAN de datos por cada conmutador de acceso para que cada uno de ellos disponga de un segmento de red de direcciones IP y conectar cada uno de esos conmutadores a la capa de distribución mediante un enlace de capa 3. Si se implementan diferentes VLANs, la conexión con la capa de distribución suele hacerse mediante enlaces troncales 802.1Q que transporten dichas VLANs y también se suele configurar el protocolo Spanning Tree (STP), con una instancia por VLAN, para proveer de balanceo de carga y redundancia.

1.1.2 Capa de distribución

En un diseño de red en una organización, la tarea única y exclusiva de la capa de distribución es actuar como puente entre la capa de acceso y la capa de núcleo. Tanto la capa de acceso como la capa de núcleo son capas especializadas, pero la capa de distribución puede servir a diferentes propósitos, como por ejemplo:

- Punto de agregación de todos los conmutadores de acceso.
- Provisión de políticas en el bloque de capas acceso-distribución.
- Participación en el enrutamiento de la capa de núcleo.

Los conmutadores de capa de distribución deben aislar la capa de acceso, en el sentido de que si surge un problema en dicha capa, este no afecte a la capa de núcleo. Los conmutadores de capa de distribución deben encargarse de limitar la conexión de las diferentes VLANs cuyo tráfico tiene origen en la capa de acceso.

La capa de distribución permite conectar diferentes localizaciones a la capa de núcleo manteniendo un alto rendimiento. Para esto, la capa de distribución puede sumarizar las rutas que provienen de la capa de acceso. En muchos diseños de red, los conmutadores de capa de distribución actúan como puertas de enlace para los dispositivos de la capa de acceso y ejecutan protocolos de enrutamiento dinámico para comunicarse con los dispositivos de la capa de núcleo, ya sean conmutadores o enrutadores.

Para ofrecer una alta redundancia en la capa de distribución, se pueden configurar conmutadores virtuales en la red. Dos conmutadores interconectados entre sí con enlaces redundantes se pueden configurar para que operen en conjunto como un único conmutador virtual, de modo que se ofrece balanceo de carga y respuesta inmediata ante el fallo en el funcionamiento de alguno de ellos.

1.1.3 Capa de núcleo

El diseño de la capa de núcleo es el más simple, pero a la vez es el más importante, ya que la capa de núcleo es la más crítica en un diseño de red jerárquico. La capa de núcleo interconecta todas las localizaciones y segmentos de red separados, así que debe ser diseñada para proveer un alto rendimiento y una alta disponibilidad. La capa de núcleo no debe poseer dispositivos finales directamente conectados.

La capa de núcleo debe proveer de una alta redundancia y debe responder ante un fallo en la red con la mayor rapidez posible, para lo que se recomienda una arquitectura de malla completa. La arquitectura de malla completa, o full mesh, especifica que en un grupo de conmutadores, todos deben poseer una conexión directa con todos los demás, así se asegura una redundancia completa.

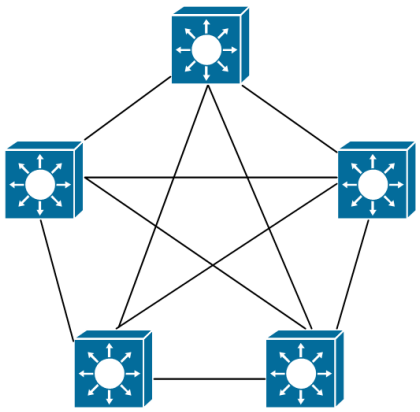


Figura 110 Arquitectura de malla completa

Para las pequeñas y medianas empresas (PYMEs), un diseño de red jerárquico de tres capas puede ser excesivo. Para solucionar esto, en la mayoría de las PYMES, u organizaciones de pequeño tamaño, se diseña una jerarquía de dos capas, donde la capa de núcleo y distribución se agrupan en otra capa denominada capa de núcleo colapsado, que implementa todas las funcionalidades de ambas capas mencionadas. Con esta aproximación se reducen costes pero también se pierde escalabilidad.

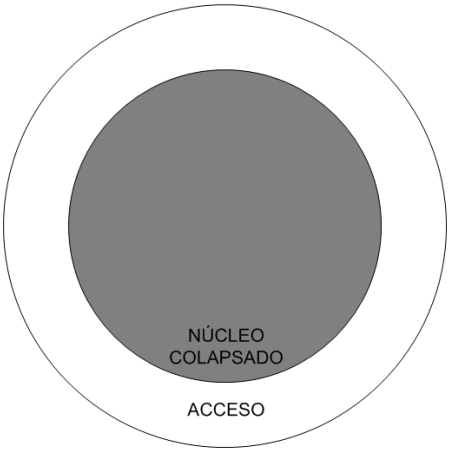


Figura 111 Jerarquía de red en dos capas con núcleo colapsado

1.2 Diseño modular de redes

El diseño funcional de redes divide una red empresarial en áreas funcionales diferenciadas, las cuales se dividen internamente en diferentes módulos. Dicha separación ofrece ventajas a la hora de solucionar problemas y ofrece flexibilidad en el diseño de la red. El diseño modular divide la red en las siguientes áreas funcionales:

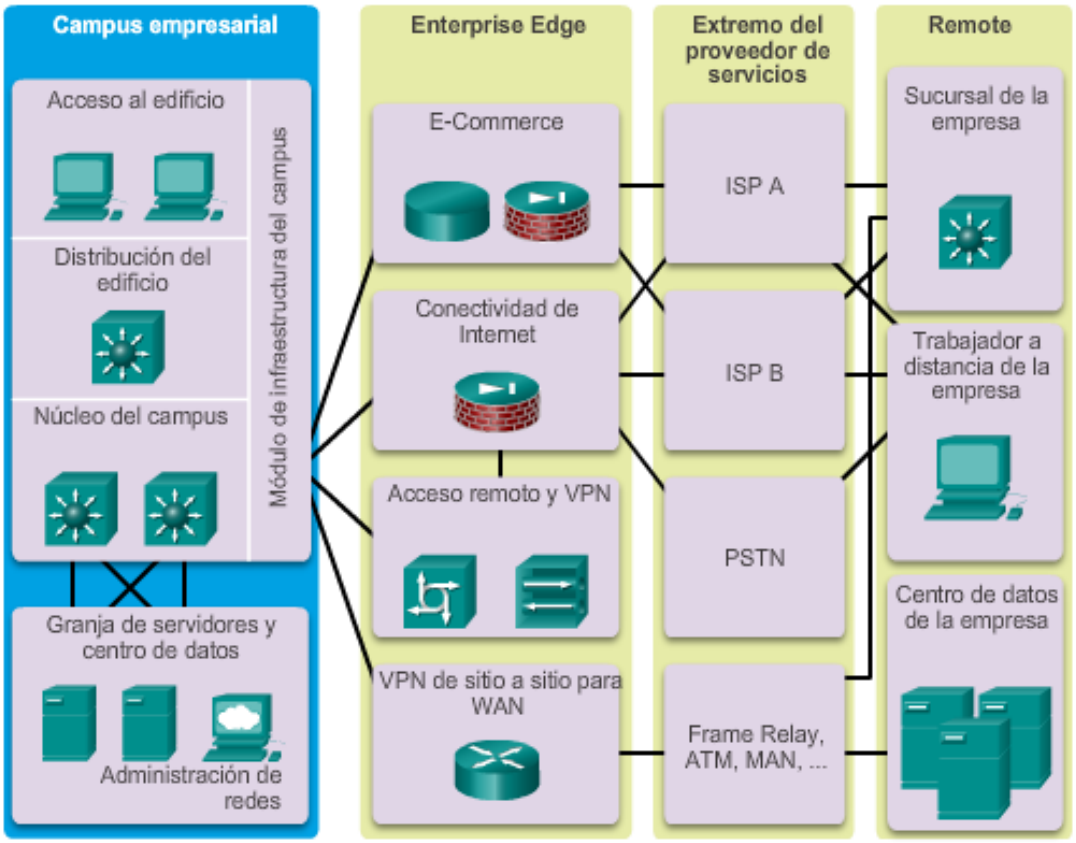


Figura 112 Áreas funcionales del diseño modular de la red de una organización

1.2.1 Campus de la organización

Un campus es una localización amplia que suele usarse como sede principal de una organización que normalmente incluye el módulo de la infraestructura de red y el módulo de la granja de servidores y centro de datos.

1.2.1.1 Módulo de infraestructura de red

Utilizando el concepto de diseño de red jerárquica, el módulo de infraestructura de red se compone de las capas de acceso, distribución y núcleo de la red. Este módulo interconecta todos los dispositivos finales con los equipos que actúan como borde de la organización y con la granja de servidores y centros de procesamiento de datos.

1.2.1.2 Módulo de centro de datos

En un diseño habitual de red en una organización, el centro de datos ofrece soporte para la administración de la red, como por ejemplo, monitorización de la red, solución de problemas, entro otros.

Este modulo de centro de datos también incluye los servidores internos que ofrecen servicios a todos los dispositivos finales de la organización, como DNS, aplicaciones, impresión, etc. Como el acceso a estos servidores es muy importante, se recomienda que se conecte cada servidor a dos conmutadores para ofrecer alta redundancia, que también se interconectarán de manera redundante a los conmutadores de capa de núcleo del módulo de infraestructura de red.

1.2.2 Área de borde de la organización.

La infraestructura de borde de la organización agrupa la conectividad de varios dispositivos externos al campus de la organización y enruta el tráfico hacia la capa de núcleo de la infraestructura de red interna. Los módulos pertenecientes al área de borde de la organización ofrecen funcionalidades de seguridad que securizan los recursos de la organización cuando se producen conexiones con redes públicas y/o Internet.

Estos módulos pertenecientes al área de borde de la organización conectan con el núcleo de la infraestructura de red directamente o mediante un módulo de borde de distribución.

1.2.2.1 Módulo de E-Commerce

Todas las transacciones que pertenecen a operaciones y servicios de comercio electrónico, transitan por este modulo, proveyendo seguridad, escalabilidad y alta disponibilidad para todo el diseño de comercio electrónico.

Dentro del módulo de E-Commerce se suelen encontrar sistemas como servidores web, servidores de aplicaciones, servidores de bases de datos, cortafuegos, sistemas en red de prevención de intrusiones y conmutadores multicapas con módulos de prevención de intrusiones.

1.2.2.2 Módulo de conectividad de Internet

El módulo de conectividad de Internet provee a los usuarios internos de la organización de la posibilidad de acceder a servicios externos de Internet como HTTP, FTP, SMTP y DNS. Este módulo también provee a los usuarios internos de acceso a los servidores públicos de la organización.

Para el acceso de usuarios remotos a la organización, el modulo de conectividad de Internet acepta conexiones VPN, que luego redirigirá al módulo VPN, para que la conexión tenga lugar de manera exitosa.

Los sistemas que se pueden encontrar en el módulo de conectividad de Internet son servidores de correo SMTP, servidores DNS, servidores públicos FTP y HTTP, cortafuegos y enrutadores frontera con Internet.

1.2.2.3 Módulo de WAN, MAN y VPN sitio a sitio

El módulo de WAN, MAN y VPN sitio a sitio utilizan varias tecnologías WAN y MAN más recientes para enrutar el tráfico entre los sitios remotos y la infraestructura central de la organización, tales como SONET y SDH, DSL, MLPS, Metro Ethernet y VPNs de proveedores de servicio.

1.2.2.4 Módulo de acceso remoto y VPN

El módulo de acceso remoto y VPN es el encargado de la gestión integral de todo el tráfico de acceso remoto así como del tráfico VPN que es redirigido desde el módulo de conectividad de Internet que pertenece a conexiones de usuarios o sucursales remotos.

Entre los dispositivos que se pueden encontrar en el módulo de acceso remoto y VPN se encuentran dispositivos de seguridad Cisco ASA, cortafuegos, aplicaciones NIPS y concentradores de acceso a Dial-in.

1.2.3 Área del proveedor de servidos (ISP)

Todos los módulos incluidos en el área del proveedor de servicios (ISP) representan la infraestructura de conexión con los ISP.

1.2.3.1 Módulo ISP

El módulo ISP representa la conexión a la red de un ISP. Una organización se puede conectar a un ISP para obtener un acceso básico a Internet o para ofrecer conectividad remota a sucursales o usuarios remotos.

1.2.3.2 Módulo PSTN

El módulo PSTN (Red de Telefonía Conmutada Pública) representa la infraestructura dialup para acceder a la red de la organización utilizando ISDN, y tecnologías analógicas y móviles. Este módulo también puede ser utilizado por una organización para crear conexiones WAN de respaldo que se usan bajo demanda y se desconectan después de un tiempo de no utilización.

1.2.3.3 Módulo Frame Relay y ATM

El módulo Frame Relay y ATM incluye todas las tecnologías WAN para conexiones permanentes con localizaciones remotas que se construyen utilizando Frame Relay y/o ATM.

1.2.4 Área remota

Los módulos pertenecientes al área remota describen los componentes y funcionalidades necesarias para la conexión remota de sucursales, centros de datos y trabajadores pertenecientes a la organización.

1.2.4.1 Módulo de sucursal remota

El módulo de sucursal remota permite extender la organización mediante la provisión a sucursales remotas de una arquitectura de red segura, redundante y flexible. Los usuarios de una sucursal remota deben acceder a todos los recursos internos de una organización de igual modo que lo harían si estuvieran en la sede central de dicha organización. Este módulo puede utilizar servicios como VPNs, PSTN, videoconferencias, etc.

Normalmente, el módulo de sucursal remota utiliza una versión simplificada de la infraestructura de red del campus de la organización.

1.2.4.2 Módulo de centro de datos remoto

El módulo de centro de datos remoto tiene una arquitectura similar a la desplegada en el módulo de centro de datos del campus de la organización. Los componentes que incluyen un módulo de centro de datos remoto son:

- Infraestructura de red con conmutación Gigabit o 10 Gigabit.
- Servicios interactivos de almacenamiento, de computación, de seguridad y de optimización de aplicaciones.

Todos los centros de datos remotos deben disponer de una conexión WAN de alta disponibilidad.

1.2.4.3 Módulo de trabajadores remotos

El módulo de trabajadores remotos provee de conectividad a trabajadores de una organización que estén distribuidos geográficamente para que puedan explotar los recursos de la organización desde sus casas, desde un hotel, etc.

Las oficinas centrales de la organización son las encargadas de ofrecer seguridad y alta disponibilidad a las conexiones remotas de los trabajadores. Normalmente, la administración de dichas conexiones se realiza desplegando un sistema automático de administración para que los dispositivos que proveen de conexión se mantengan actualizados y configurados según las políticas de la empresa.

2 Monitorización de Seguridad de Redes (NSM)

La Monitorización de Seguridad de Redes (NSM) se define como la recolección, análisis y notificación de indicaciones y advertencias para detectar intrusiones y responder a ellas.

Lo primero es comprender a qué se refieren los términos "indicadores y advertencias". Los **indicadores** son aquellas acciones observables o discernibles que confirman o deniegan las capacidades o intenciones del enemigo, por ejemplo, un pico en el tráfico ICMP, una conexión inusual de un servidor, etc. Los IDS denominan **alertas** a estos indicadores. Lo preferible es que todas las alertas correspondan a un ataque real, pero esto es imposible ya que los IDS no poseen la **información de contexto**, es decir, la información que ayuda a comprender la naturaleza de un suceso con respecto a todos los demás aspectos del entorno de una organización. Por ejemplo, un test de penetración legítimo sin previo aviso a los administradores de red puede provocar un falso positivo. La adquisición de la información de contexto depende del administrador de red. Las **advertencias** son los resultados de la interpretación de los indicadores por parte de los administradores de red. Al proceso de la monitorización estratégica del tráfico de red destinada a apoyar la detección y verificación de intrusiones se le denomina **I&W digital**.

La **recolección** de los indicadores es una labor de los IDS. El **análisis** de los indicadores es responsabilidad de las personas y, aunque algunos IDS están capacitados para tomar decisiones en función de unas reglas preestablecidas, siempre se necesita la interpretación de un especialista para proporcionar información de contexto. La **notificación** es el acto de poner la información en conocimiento de quienes tiene la autoridad, la responsabilidad y la capacidad de responder a incidentes potenciales.

Siempre hay que tener en cuenta que la prevención tiene una alta probabilidad de resultar insuficiente en algún punto determinado. Cuándo la prevención falla, es importante recabar la máxima cantidad de información posible sobre la intrusión, es decir, la cantidad de información que nos permita responder a: **¿Qué ha hecho el intruso?**, **¿cuándo lo hizo?**, **¿sigue teniendo acceso el intruso?**, **¿qué gravedad puede tener el compromiso?** Esta información es vital a la hora de definir un curso de acción que permita verificar la seguridad del sistema tras los arreglos pertinentes. La mayoría de los despliegues de sistemas IDS suele fallar debido a que los administradores de red no leen los registros que estos sistemas generan. Un IDS no es un elemento de respuesta activa ante los intentos de intrusión, un IDS sólo notifica, y es responsabilidad del administrador continuar la cadena de actuación para el correcto tratamiento del intento de intrusión.

Cabe la posibilidad de que una intrusión pueda pasar desapercibida para un sistema NSM, pero la labor de un NSM no sólo consiste en la detección de intrusiones. Un sistema NSM también debe recolectar toda la información posible de la red para ayudar a los analistas a comprender de manera más efectiva el alcance de las intrusiones.

Los sistemas NSM también tienen limitaciones. Recolectar todos y cada uno de los paquetes que transitan una red podría haber sido algo factible hace algunos años, pero las características actuales de las redes y las previsiones de crecimiento hacen que interpretar toda la cantidad de información que es posible recoger sea una tarea muy complicada. Sin

embargo, se recomienda recolectar todos los paquetes independientemente de la capacidad de análisis disponible, ya que nunca se sabe donde un intruso podría haber dejado algún rastro o cualquier tipo de dato. La cantidad de información que se puede recolectar está limitada por el ancho de banda de la red, la capacidad de almacenamiento, la potencia de procesamiento y las leyes y políticas locales. Además, las necesidades de almacenamiento pueden variar según las características de la organización, por ejemplo, una entidad bancaria necesitará recolectar más datos que una pequeña empresa.

2.1 Despliegue de un NSM

Para que un sistema NSM pueda recolectar el tráfico de una red para el posterior análisis por parte de un especialista, hay que asegurar que el sistema NSM sea capaz de ver todo ese tráfico que transita la red que debe monitorizar. Antes de analizar el tráfico de red, se deben definir las clases de atacantes que pueden lanzar un intento de intrusión contra una red:

Clase	Origen del atacante	Origen del ataque
1	Externo	Internet
2	Externo	Segmentos inalámbricos
3	Interno	Redes locales cableadas
4	Interno	Segmentos inalámbricos

Tabla 21 Clasificación de ataques

La capacidad para visualizar el tráfico que transita una red depende del despliegue de plataformas de monitorización en la red, o sensores. Un **sensor** es un dispositivo que recolecta y analiza tráfico de red con el propósito de identificar sucesos sospechosos. En el proceso de despliegue de sensores en una red ya construida, hay que estudiar las diferentes zonas que la red posee. Por ejemplo, analizando la siguiente red:

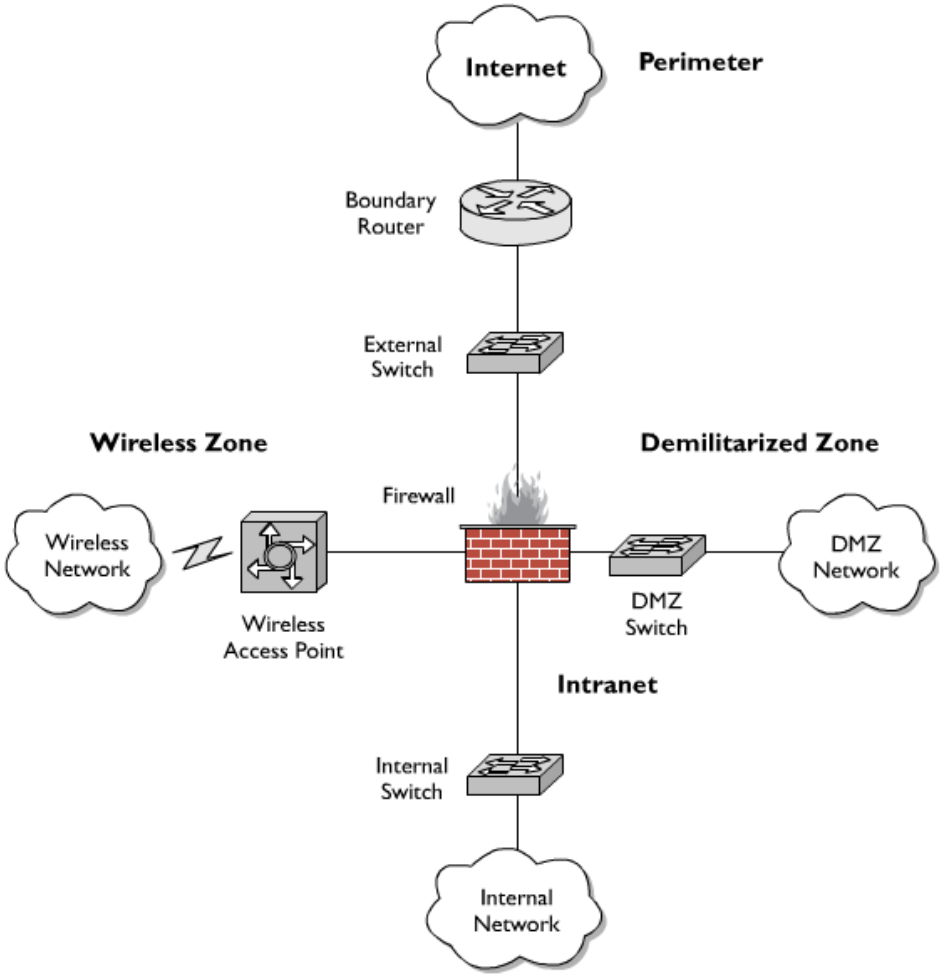


Figura 113 Zonas de una red conmutada

Podemos apreciar que la red posee cuatro zonas de monitorización. Una zona de monitorización es una ubicación cuyo tráfico comparte los mismos privilegios, basados en el nivel de confianza que le otorga un experto en seguridad. Las zonas de monitorización, delimitadas por el cortafuegos central, son:

- **Zona perimetral**: Zona que abarca el segmento de red desde el cortafuegos hasta Internet.
- **Zona desmilitarizada (DMZ)**: Zona que abarca el segmento de red conectado a la interfaz DMZ del cortafuegos.
- **Zona inalámbrica**: Zona que abarca todas las máquinas conectadas que poseen conectividad inalámbrica a la red.
- **Zona interna o Intranet**: Zona que abarca todo el segmento de red conectado a la interfaz interna del cortafuegos.

Cada una de estas zonas posee sistemas que pueden ser susceptibles de ser víctimas de ataques de cualquiera de las clases descritas anteriormente. Veamos las características propias de cada una de las zonas.

2.1.1 Zona perimetral

La zona perimetral es la zona ideal para desplegar sensores cuyo objetivo es monitorizar ataques de clase 1, es decir, ataques generados por atacantes externos procedentes de Internet. La zona perimetral es la zona de menos confianza, ya que es la zona donde la empresa tiene menos control de todo lo que sucede en ella. Un despliegue de un sensor en una zona perimetral ofrece un enfoque amplio sobre la zona destino del ataque de clase 1, ya sea la DMZ, la zona inalámbrica o la Intranet.

La colocación de un sensor en la zona perimetral no ofrece visibilidad sobre el tráfico que no abandona una zona determinada diferente a la perimetral, sin embargo, si un ataque tiene origen en cualquiera de las zonas y tiene como destino Internet, si se puede detectar por los sensores de la zona perimetral.

Debido a que la zona perimetral es el punto de entrada de Internet a la red de la organización, todo el tráfico proveniente de Internet que transita esa zona todavía no ha sido filtrado por ningún cortafuegos, lo que conlleva una gran cantidad de información a analizar por el analista.

2.1.2 Zona desmilitarizada (DMZ)

Los sensores que se despliegen en una zona desmilitarizada tienen como objetivo vigilar las máquinas que usualmente residen en este tipo de zona, como puede ser un servidor web, un servidor de correo, un servidor FTP, etc. Lo más normal en una red que posea una zona desmilitarizada es que el cortafuegos que actúa como delimitador de zonas limite el tráfico que entra en la DMZ, por lo que los sensores desplegados en esta zona registrarán menos actividad.

La gran dificultad que se encuentran los sensores desplegados en una DMZ es la recolección de tráfico encriptado que pueden generar conexiones a equipos de la DMZ como un servidor web que utiliza SSL. Los equipos situados en una DMZ son de confianza media ya que están directamente controlados por la organización, pero al ser accesibles desde internet, son susceptibles de sufrir ataques.

2.1.3 Zona inalámbrica

Todos los equipos conectados en la zona inalámbrica, a efectos de confianza, se tratan como los equipos que se encuentran conectados a Internet y acceden a la organización a través de la zona perimetral.

Los atacantes externos provenientes de segmentos inalámbricos (clase 2) pueden pertenecer a dos subcategorías:

- Atacantes que acceden a segmentos inalámbricos mal configurados.
- Espías corporativos que intentan sustraer propiedad intelectual.

2.1.4 Zona interna o Intranet

Los equipos conectados a la Intranet de la organización son los equipos que más confianza disponen. No se debe permitir el acceso desde Internet a los equipos de esta zona, a no ser que la conexión se realice mediante una VPN.

Los ataques lanzados desde la Intranet son los de clase 3, es decir, son los ataques cuyos atacantes tienen el estatus de personal interno de la organización. Lo más usual es que un atacante externo utilice los privilegios proporcionados por la organización para realizar un acceso autenticado pero no legítimo a información privilegiada, para su posterior copia en dispositivos de almacenamiento masivos, como dispositivos USB o tarjetas SD. Los atacantes de clase 4 utilizan la misma metodología de ataque.

Otra dificultad para los sensores desplegados en una Intranet es la complejidad de la topología de red de la organización y la elevada cantidad de tráfico que transita la red. Lo normal es que las computadoras con un nivel similar de importancia se agrupen en conjuntos delimitados por un cortafuegos y se despliegue un sensor que monitorice el tráfico que sale del cortafuegos.

2.2 Acceso al tráfico de la red

A la hora de recolectar el tráfico que transita las diferentes zonas de una red, disponemos de diferentes medios técnicos diseñados para tal fin. Un sistema NSM no está diseñado para interferir en el tráfico, sino que su despliegue debería ser transparente para todo el tráfico que transita la red. Un sensor desplegado en la red no debe generar tráfico en las interfaces conectadas a la red a monitorizar, que están configuradas en modo promiscuo para aceptar todos los paquetes entrantes por dicha interfaz.

En redes cableadas hay diferentes formas de recolectar el tráfico que transita dichas redes:

- Puertos espejo.
- TAPs.
- Dispositivos en línea.

2.2.1 Puertos espejo

Un puerto espejo es un puerto destinado a la monitorización del tráfico que conmuta un conmutador de calibre industrial, es decir, un conmutador que se puede administrar de manera remota. Un puerto espejo refleja todo el tráfico que recibido en otros puertos. El sensor que formará parte del sistema NSM se conecta a dicho puerto espejo.

Hay que tener en cuenta el ancho de banda del que dispone el puerto espejo. Si se quieren reflejar 10 puertos de un conmutador que trabajan a 100 Mbps, el puerto espejo deberá ser como mínimo un puerto Gigabit Ethernet (1000 Mpbs). En el caso de que el ancho de banda del puerto espejo sea menor, una posible congestión de tráfico en los puertos reflejados puede provocar pérdida de datos en el puerto espejo.

Cuando se captura tráfico en un puerto espejo se descarta toda la información sobre VLAN, es decir, el tráfico es idéntico a como lo visualizarían el equipo destino o el equipo origen.

Los puertos espejo se utilizan con frecuencia en las organizaciones debido a que los dispositivos ya instalados con anterioridad pueden proveer estas funcionalidades.

2.2.2 TAPs

Un TAP, o puerto de acceso para pruebas, es un dispositivo de red diseñado específicamente para monitorización de tráfico de red. Un TAP provee a un sensor de un puerto de conexión permanente de monitorización pasiva.

Los TAPS suelen ofrecer cuatro puertos. Dos puertos se utilizan para la replicación de la conexión punto a punto anterior a la instalación del TAP y los otros dos puertos se utilizan para la monitorización del tráfico que transita dicho enlace punto a punto. Un TAP respeta el modo de operación full dúplex del enlace existente en los dispositivos entre los que se sitúa el TAP. Un puerto de monitorización ve el tráfico entrante mientras que el otro ve el tráfico saliente. El hecho de que el flujo de tráfico se vea separado en dos puertos diferentes puede acarrear problemas si las necesidades de la monitorización requieren obtener información sobre el flujo completo. Para evitar este problema, tenemos cuatro alternativas:

- Recopilar el tráfico en dos NICs diferentes y simular una única NIC virtual para el software de monitorización
- Recopilar el tráfico por separado y utilizar el software de monitorización para crear un flujo único
- Enviar las líneas de monitorización del TAP a un conmutador y conectar el sensor a un puerto espejo.
- Desplegar hardware especializado para combinar ambos flujos en uno solo.

Cabe resaltar que no se debe utilizar un concentrador para combinar el tráfico procedente de un TAP, debido a las colisiones que provocaría la entrada simultánea de paquetes en el concentrador enviados desde el TAP.

Puede que el hecho de que un TAP ofrezca dos salidas de monitorización, una para cada sentido de la comunicación full dúplex entre dos dispositivos, pueda resultar algo complicado para su despliegue en una red. Recientemente, se han comercializado TAPs que sólo ofrecen una salida para la monitorización del tráfico. A estos TAPs se los denomina *Agregadores de Puertos*. Este tipo de TAPs ofrecen la posibilidad de conectar un sensor con una sola NIC al TAP y disponer al instante de toda la información del flujo de conexión entre dos dispositivos.

Los TAPs no añaden un punto adicional de fallo en la red, como hacían los concentradores. Un TAP, en el caso de que falle su alimentación eléctrica, seguirá permitiendo el paso de tráfico de red en las interfaces dispuestas para la simulación de un enlace punto a punto.

La desventaja de utilizar TAPs es el coste que supone su adquisición. Si se dispone de los recursos necesarios para su despliegue, los TAPs son la mejor opción.

2.2.3 Dispositivos en línea

Un dispositivo en línea se considera un servidor especializado o dispositivos hardware cuya flexibilidad y complejidad sean mayores que los de un concentrador, un puerto espejo y un TAP. Se puede optar por utilizar un cortafuegos para recolectar todo el tráfico por una

interfaz diferente, aunque se incumpliría el principio de separación de tareas, ya que un cortafuegos debe tener como único propósito el control de acceso.

Un dispositivo en línea suele colocarse como un puente transparente, es decir, que dejen pasar el tráfico de red sin alterar el encabezado de los paquetes. Un dispositivo en línea suele ser un ordenador. Esto ofrece la ventaja de que ese mismo ordenador que recolecta el tráfico puede ejecutar software de monitorización, como Snort.

Las desventajas de utilizar dispositivos en línea son:

- Añaden otro punto de fallo a la red, al igual que los concentradores.
- Añaden latencia a las conexiones.
- El dispositivo puede ser atacado y verse comprometido.

2.3 Arquitectura de un sensor

Un sensor es el sistema que alberga las aplicaciones NSM. A la hora de desplegar un sensor, hay que tener en cuenta que requerimientos de hardware y de sistema operativo existen en el sistema NSM.

2.3.1 Hardware

Lo usual es que un sensor utilice hardware de Intel debido al bajo coste que supone su adquisición y a la gran variedad de herramientas que ofrece. Las velocidades y capacidades de almacenamiento del resto del hardware del sensor dependen de las características físicas de la red.

A continuación se definen los estándares de comunicaciones digitales que suelen encontrarse en enlaces de red:

Nombre	Ancho de banda (Mbps)	Aplicación
T-1	1.544	Pequeñas empresas
T-3	44.736	PYMES
OC-3	155.52	Grandes empresas y conexiones de ISPs
OC-12	622.08	Conexiones de ISPs
OC-48	2488.32	Conexiones Backbone lentas
OC-192	9.953.28	Conexiones Backbone rápidas

Tabla 22 Estándares de comunicaciones digitales

Según los estándares de comunicaciones digitales existentes en la red que el sensor va a monitorizar, se definen los siguientes requerimientos de hardware:

Componente	Línea T-1 poco usada o inferior	Línea T-1 muy usada – Línea T-3 poco usada	Línea T-3 muy usada o superior
CPU	Pentium II 300 Mhz	Pentium III 750 Mhz	≥Pentium IV I GHz
RAM	256 MB	512 MB	≥ 1 GB
HDD	20 GB	80 GB	≥ 240GB
Bus PCI	32 bits	32/64 bits	≥ PCI-X o Express

Tabla 23 Requerimientos hardware de un sensor NSM

Aparte de estas recomendaciones sobre las características del hardware del sensor, lo habitual es que dicho sensor posea una NIC para administración y una o más NICs para monitorización.

2.3.2 Sistema operativo

La recomendación general es utilizar el sistema operativo FreeBSD, aunque cualquier sistema Linux ofrece las herramientas para compilar todas las aplicaciones NSM necesarias.

Los sistemas Windows no son adecuados para la monitorización debido a la baja confianza que generan a la hora de protegerse contra ataques externos y las reducidas capacidades de modificación del sistema que ofrecen. Un sistema UNIX puede modificarse de una manera tan exhaustiva que reduzca al máximo los elementos innecesarios del sistema operativo para aumentar al máximo el rendimiento del sensor.

2.4 Administración de los sensores

Puede darse el caso, de que los datos que recoge un sensor sólo estén disponibles en él y no en otra plataforma centralizada de recolección de datos NSM. Debido a esto, los administradores de red necesitan ser provistos de algún método de conexión al sensor. A continuación se exponen los tres métodos más conocidos para el acceso a un sensor:

- Acceso por consola
- Acceso remoto en banda
- Acceso remoto fuera de banda

2.4.1 Acceso por consola

El acceso por consola, ya sea a través de un teclado o de un cable serie, es la manera más segura de administración se un sensor NSM. Sólo se utiliza una interfaz de monitorización y las aplicaciones con arquitectura cliente/servidor ejecutan tanto el cliente como el servidor en el mismo sensor.

Esto es conveniente para organizaciones pequeñas dónde el administrador de red está situado cerca del sensor, pero en organizaciones grandes donde los sensores pueden estar ubicados a gran distancia, el acceso por consola no es una opción.

El hecho de la existencia de una limitación de acceso por consola no evita que un atacante pueda intentar comprometer el sensor a través de la interfaz de monitorización.

2.4.2 Acceso remoto en banda

Este tipo de acceso proporciona al administrador de red la posibilidad de conectarse al sensor utilizando la infraestructura nativa de la organización. La conexión del administrador con el sensor transita la misma red que el resto de datos de la organización (correos, ficheros, etc.) Aunque esta información puede estar encriptada, sigue compartiendo medio físico con el resto de datos.

Si el sensor se encuentra en una sede remota transmiten sus datos a través de internet utilizando VPNs, pero si el sitio remoto queda incomunicado, el sensor también quedará incomunicado.

La desventaja de basarse en una administración por acceso remoto en banda es que, si las configuraciones de Secure Shell, de VPN u otro cualquier aspecto de la red son incorrectas, el sensor remoto quedará aislado y se requerirá de acceso físico al mismo, lo que puede suponer un viaje hasta el mismo.

2.4.3 Acceso remoto fuera de banda

Este tipo de acceso implica que la administración de un sensor reside en el uso de canales de comunicación independientes de la infraestructura nativa de la organización.

Por ejemplo, si se tiene miedo de perder la conexión con un sensor a través de Internet, se puede dotar al sensor de un módem telefónico y conectar dicho módem a una línea telefónica ya preparada, para poder acceder al sensor con una simple llamada de teléfono.

2.5 Datos a monitorizar

A la hora de recolectar el tráfico que transita una red para su posterior análisis por parte de un especialista, se debe aclarar que hay varios tipos de datos que una plataforma NSM puede recolectar:

- Datos de contenido completo.
- Datos de sesión.
- Datos estadísticos.
- Datos de alerta.

2.5.1 Datos de contenido completo

Cuando hablamos de la recolección de datos de contenido completo nos referimos a la recolección completa de todos y cada uno de los bits con sentido de los paquetes que transitan la red. Los datos de contenido completo ofrecen a los analistas la posibilidad de derivar de su análisis el resto de tipos de datos: sesión, estadísticos y de alerta. Los datos de contenido completo ofrecen dos características esenciales: **granularidad** y **relevancia para la aplicación.**

La **granularidad** se refiere a la recolección completa de todos los paquetes que transitan una red y todos sus datos que poseen algún sentido. Este tipo de recolección es muy útil cuando un atacante realiza un ataque modificando el final de las cabeceras de algún protocolo de comunicación, siendo indetectable para cualquier plataforma que sólo recolectara los encabezados de los paquetes.

La segunda característica importante de los datos de **contenido completo** es la relevancia para la aplicación. Esto se refiere a que los en datos de contenido completo también se almacena toda la información de capas superiores a la capa de transporte.

Para recolectar datos de contenido completo disponemos de diversas herramientas como **Tcpdump**, **Snort** y **Wireshark.**

La desventaja de la recopilación de los datos de contenido completo es la gran capacidad de almacenamiento necesaria para archivar todos los paquetes que transitan una red. Por ejemplo, recolectar 14 días de tráfico en una red con ancho de banda de 6 Mbps puede llegar a ocupar 75GB, lo cual puede ser manejable, pero si el ancho de banda de la red es de 100 Mbps, el tamaño de los datos sube hasta 1200 GB, lo que ya empieza a ser un tamaño excesivo. Otra desventaja es la cantidad de análisis que requiere este tipo de datos, ya que se recolectan todos los paquetes de la red y para detectar un ataque hay que analizarlos uno a uno. Al final, la recolección de datos de contenido completo dependerá de las necesidades

de la organización y de los recursos de los que se disponga para su análisis y almacenamiento.

2.5.2 Datos de sesión

Los datos de sesión representan el resumen de una conexión entre dos sistemas. Una sesión, también denominada flujo, corriente o conversación, es un resumen de un intercambio de paquetes entre dos sistemas.

Normalmente, las conexiones mediante TCP, o algún otro protocolo orientado a conexión, son las más susceptibles de aparecer representadas en datos de sesión ya que poseen fases claramente delimitadas en sus conexiones: inicial, intermedia y fila. Los protocolos no orientados a conexión, como UPD e ICMP, son más difíciles de representar como una sesión.

El núcleo de la información que almacena una plataforma NSM que recolecta datos de sesión son los siguientes elementos:

- Dirección IP de origen.
- Puerto de origen.
- Dirección IP destino.
- Puerto de destino.
- Sello de tiempo (normalmente suele ser el inicio de la conexión)
- Cantidad de información intercambiada.

Cuándo en una red es imposible la captura de los datos de contenido completo, ya sea por qué no disponemos de los recursos necesarios o por qué no resulta estrictamente necesario, la recolección de datos de sesión es la siguiente mejor opción, ya que necesitamos menos capacidad de almacenamiento, a costa de recolectar menos información.

Existen dos métodos principales de recolección de datos de sesión. El primero método consiste en recolectar todo, es decir, recolectar datos de contenido completo y luego resumirlos para generar los datos de sesión. Este método añade la desventaja que tenía la recolección de datos de contenido completo, en lo referente a capacidad de almacenamiento. El segundo método consiste en priorizar el almacenamiento de los datos de sesión. Esto se consigue mediante el análisis del tráfico que una herramienta NSM puede visualizar para, posteriormente, sólo almacenar los datos de sesión de ese tráfico. El inconveniente de esto es que la herramienta NSM debe ser capaz de ver todo el tráfico posible de la red.

A la hora de recoger datos de sesión, disponemos de varias herramientas disponibles:, por ejemplo, **Netflow**, **Fprobe** y **Argus.**

2.5.3 Datos estadísticos

Los datos estadísticos son el siguiente salto en lo referente a la granularidad en la recolección del tráfico que transita la red de una organización. Para el resumen de la colección del tráfico de la red se utiliza la estadística descriptiva. Si se analiza el tráfico que transita una red durante un periodo determinado se puede definir un comportamiento básico para detectar cualquier tipo de desviación del mismo. La desviación de la normalidad

puede ser provocada por una intrusión o un simple uso puntual de más recursos de la red, eso ya queda a interpretación del analista que esté detrás de la administración de la red.

Hay dos conjuntos de herramientas que se pueden utilizar para recolectar datos estadísticos, clasificadas según el momento en el que realicen la recolección. El primer conjunto de herramientas recolectan y muestran datos estadísticos en tiempo real. Esto es útil para la detección de ataques por denegación de servicio (DoS), equipos que acaparan mucho ancho de banda y para monitorizar sesiones en tiempo real. Estas herramientas son **Tcpdstat** e **IP Accounting**. El segundo conjunto de herramientas realizan la recolección de datos estadísticos sobre datos recolectados con anterioridad. Normalmente se utilizan para comparar las estadísticas pasadas de la red con las actuales y para detectar tendencias. En este conjunto de herramientas se incluyen **MRGT y Ntop**.

2.5.4 Datos de alerta

Hasta ahora, todos los datos presentados que permiten recolectar las herramientas NSM dependen del criterio y el análisis por parte de un especialista para determinar qué datos están relacionados con intrusiones o que datos son normales en el uso diario de una red. Existen unas herramientas NSM denominadas Sistemas de Detección de Intrusiones (IDS), que se encargan de analizar los datos para alertar, con la mayor precisión y veracidad posible, de cuando se está llevando a cabo un intento de intrusión.

Los sistemas de detección de intrusiones se explican con profundidad en el siguiente apartado.

3 Sistema de detección de intrusos IDS

3.1 Teoría general

Debido a la creciente dependencia de Internet, de las Intranet y del acceso a Extranets, la intrusión en sistemas de usuarios no autorizados es un problema creciente. Una intrusión es un acceso no autorizado o un intento del mismo a un ordenador o un sistema de información. La detección de intrusiones es el proceso de identificación de un intento de intrusión que se está realizando en el momento o se llevó a cabo con anterioridad.

Un Sistema de Detección de Intrusos (IDS) es un sistema de que monitoriza en tiempo real la actividad de un ordenador que sea indicativa de un intento o una consecución de un acceso no autorizado de personas u otros sistemas. Acciones del sistema:

- Detecta usuarios no autorizados que intentan acceder a un sistema, comparando el comportamiento del usuario con un perfil de usuario o una política establecida por la empresa.
- Detecta eventos que indican un acceso no autorizado a la red.
- Provee funciones de control que toman decisiones en función de las alertas que el sistema detecte.

Los perfiles de usuario, o firmas, se construyen dinámicamente para cada ordenador cuando el ordenador intenta acceder al sistema por primera vez. Mediante los accesos posteriores, el perfil de usuario se actualiza. A partir de dicho perfil de usuario generado

dinámicamente, se pueden establecer las políticas de la empresa en el ámbito de la seguridad. Otra posibilidad para la generación de los perfiles de usuario es definirlos a partir de unas políticas de seguridad preestablecidas en la empresa. Los IDS también proveen de funciones de registros de auditoría, un detector de escaneado de puertos y funciones de monitorización de sesiones.

En la mayoría de sistemas de detección de intrusos, los datos son recogidos automáticamente, pero el análisis de los datos es manual.

Según el método de detección de intrusiones, los IDS se pueden clasificar en:

- **Basados en firmas.** La detección de intrusiones se realiza buscando patrones específicos, como secuencias de bytes en los paquetes del tráfico de red que se reconocen como patrones utilizados por software malicioso o malware. Si no se conoce el patrón de un ataque, es imposible detectarlo.
- **Basados en anomalías.** Los IDS basados en anomalías fueron introducidos principalmente para detectar ataques desconocidos debido a la rapidez del desarrollo de malware. La idea básica es usar aprendizaje automático para crear un modelo de actividad confiable y comparar la actividad nueva con dicho modelo. Lo más normal es que los IDS que se basan en anomalías den falsos positivos, es decir, que actividad legítima se clasifique como maliciosa.

Según el lugar donde se realice la monitorización, los IDS se pueden clasificar en:

- **Sistemas de detección de intrusiones en red (NIDS).**
- **Sistemas de detección de intrusiones en host (HIDS).**
- **Sistemas distribuidos de detección de intrusiones (DIDS).**

3.2 Sistemas de detección de intrusiones en red (NIDS)

Un NIDS monitoriza el tráfico que transita una red. Un NIDS puede localizarse en una red backbone o utilizarse como sistema de monitorización de dispositivos de red en particular como servidores, conmutadores, enrutadores, etc.

Un NIDS incluye una unidad de conexión a la red, una unidad de almacenamiento y una unidad de procesamiento.

- La unidad de conexión de red recibe los paquetes de la red.
- La unidad de almacenamiento guarda los paquetes de red recibidos, un programa de correlación de alertas y un conjunto de políticas de operación.
- La unidad de procesamiento opera un programa de alertas, un conjunto de reglas de detección y un conjunto de políticas de operación sobre los paquetes recibidos de la red.

La ventaja de un NIDS es que no tiene ningún tipo de impacto en la red que monitoriza. Un NIDS no carga en ningún sentido un equipo final y un atacante que comprometa dicho equipo no tiene por qué poder conectar con el NIDS o ni siquiera saber que existe.

La desventaja de un NIDS es el ancho de banda que requiere la monitorización. Si tenemos conmutadores con puertos de 100MB en un conmutador y queremos reflejar todo ese tráfico en un puerto concreto para monitorizar la red, el ancho de banda requerido será mucho más de 100MB.

A la hora de implementar un NIDS, tenemos varias soluciones comerciales gratuitas:

- **Snort.** Es el líder en las soluciones de código abierto de NIDS. Snort usa tanto la detección basada en anomalías como la detección basada en firmas. Ventajas:
  - El sistema es muy ligero.
  - Fácil instalación y puesta en marcha.
  - Pueden implementarse reglas propias o conectarse a una base de datos externa como Emerging Threats.
  - Amplia comunidad de usuarios y gran cantidad de recursos disponibles en línea.

  Desventajas:
  - No tiene GUI integrada, aunque existe software de terceros que soluciona este problema.
  - El procesado de paquetes puede ser lento.
- **Suricata.** Competidor directo de Snort. Suricata usa tanto la detección basada en anomalías como la detección basada en firmas. Ventajas:
  - Puede usar las reglas de Snort.
  - Soporta multi-threading y aceleración de GPU.

  Desventajas:
  - Muy dado a falsos positivos.
  - Consume muchos recursos de procesamiento y de red.
- **Bro IDS.** Este NIDS está basado en anomalías y se suele utilizar en conjunto con Snort, ya que se complementan bastante bien. Ventajas:
  - Se puede adaptar a diferentes redes y casos de uso.

  Desventajas:
  - Se requiere experiencia en programación.
- **OpenWIPS-ng.** Este NIDS está basado en firmas. Es modular y se instala en redes inalámbricas. Se compone de sensores, un servidor y una interfaz gráfica.

3.3 Sistemas de detección de intrusiones en host (HIDS)

Estos sistemas de detección de intrusos operan directamente en un sistema final y analizan el comportamiento interno de dicho sistema. Además de dichas actividades, como inspeccionar dinámicamente los paquetes dirigidos a ese equipo y los que salen de él dirigidos a la red, un HIDS puede detectar programas que acceden a recursos de manera anormal, que realizan operaciones no permitidas, por ejemplo, un procesador de texto que cambia la contraseña del sistema.

Un HIDS puede analizar el estado del sistema, su información almacenada, ya sea en la RAM o en el sistema de ficheros, y comprueba que el contenido de los mismos es el que se espera. Los HIDS se basan en el rastro de actividades que un intruso puede dejar cuando entra en un sistema. Lo más común es que un HIDS trabaje en conjunto con un NIDS.

Una desventaja de los HIDS es la dependencia del sistema operativo del sistema en el que el HIDS reside. Si tenemos equipos con diferentes sistemas operativos y queremos instalar el HIDS de una misma compañía en todos ellos, deberemos buscar aquella que ofrezca un producto que se adapte a la heterogeneidad de nuestros equipos. Otra desventaja es que los HIDS añaden carga a los dispositivos finales ya que requieren tiempo de procesamiento. Esto puede ser un problema en servidores con mucha carga de trabajo.

Un reto en la implementación de la detección de intrusiones con HIDS es mantener una red medianamente grande con muchos equipos con HIDS instalados. Los HIDS no escalan demasiado bien, y si no hay una administración centralizada de los mismos, administrar las alertas de todos ellos puede ser muy complicado.

A la hora de implementar un HIDS, tenemos varias soluciones:

- **OSSEC.** Es un HIDS gratuito y de código abierto. Realiza análisis de registros, comprobaciones de integridad, monitorización de registros de Windows, detección de rootkits, alertas basadas en tiempo y respuestas activas.
- **Open Source Tripwire.** Es un HIDS gratuito y de código abierto que analiza cambios en el sistema de ficheros.
- Para sistemas Windows, existe la posibilidad de desplegar HIDS pertenecientes a Microsoft, como **ATA** (Advanced Threat Analytics) y **Windows Defender ATP**.

3.4 Sistemas distribuidos de detección de intrusiones (DIDS)

Un sistema distribuido de detección de intrusos, o DIDS, es una combinación de sensores NIDS y HIDS distribuidos por la red, que conectan con un sistema central.

Los reportes de los ataques son generados en los sensores y se cargan en el servidor central para guardarse en una base de datos. Normalmente, los servidores que administran los sensores son diferentes de los que recogen los reportes de ataques. Si tenemos diferentes servidores de administración, se pueden adaptar las reglas que se envían a cada sensor para que la seguridad de éstos se adapte lo máximo posible a las políticas de seguridad de la red.

La información que comparten los sensores con los servidores puede transitar por una red privada exclusiva para ese cometido o puede transitar la red ya existente. Si la información viaja por la red existente, hay que añadir seguridad adicional para proteger dicha información, como encriptarla o instalar tecnologías VPN.

La ventaja del uso de un DIDS es la posibilidad de observar con un enfoque amplio todos los incidentes que ocurren en una red. Un DIDS puede ser muy difícil de diseñar y la interpretación de la información que generan los sensores requiere mucho estudio.

3.5 Tipo de información que recogen los IDS

Los tres diferentes tipos de IDS pueden recolectar diferente información en nuestra red.

3.5.1 Información específica de aplicaciones

Todos los tipos de IDS pueden recabar información de las aplicaciones que se utilizan en un equipo, como un navegador web o los datos internos de una aplicación programada por nosotros mismos.

Un NIDS puede detectar información de aplicaciones cuyo tráfico transita la red mediante protocolos como HTTP o Telnet. Si el tráfico de red que esa aplicación genera está encriptado, a la mayoría de NIDS les será imposible interpretar dicha información. Para evitar esto, los HIDS analizan dicho tráfico antes de que sea encriptado, y después, en el caso de que dicho tráfico llegue a un equipo con un HIDS instalado.

3.5.2 Información específica de los equipos

Un HIDS no tiene porque ver toda la información de un equipo, aunque son capaces de ver cambios en el sistema de ficheros y peticiones de red a una interfaz de loopback, por ejemplo.

Es muy común que un HIDS mantenga una base de datos con la información del equipo y monitorice las actividades del equipo para detectar cualquier tipo de desviación de ese comportamiento registrado.

3.5.3 Información específica de la red

La mayoría de redes tienen patrones comunes de tráfico que transita la red, por ejemplo, si tenemos un servidor de correo en nuestra red, sabemos que tráfico SMTP puede transitar la red.

Puede haber un experto en seguridad en nuestra red que genere tráfico sospechoso, pero se le debe permitir, mientras que ese mismo tráfico proveniente de otro equipo debe ser rechazado. Para conseguir esto, los NIDS deben configurarse de una manera correcta.

El mapeo de protocolos de capa 2 es una actividad que los NIDS realizan constantemente. La mayoría de IDS analizan el tráfico ARP para tener una base de datos de direcciones IP relacionadas con direcciones MAC para evitar ataques de envenenamiento de direcciones físicas. Si el tráfico atraviesa un enrutador, esta tarea resulta imposible, puesto que el enrutador sustituye las direcciones MAC fuente por la dirección MAC de su interfaz de salida del tráfico.

3.5.4 Información específica en un sistema distribuido

Toda la información anterior puede ser recabada por un DIDS, pero con la ventaja de ampliar el enfoque de recolección a la amplitud general de toda la red, no sólo a una subred.

La ventaja es que el tráfico que no parece malicioso, como la realización de la copia de seguridad de un servidor, puede descubrirse como un ataque coordinado de copia de toda la información si se tiene una visión general de todo lo que ocurre en la red.

La desventaja es que la cantidad de información que recoge un DIDS es inmensa, y si no se tiene las herramientas adecuadas para su interpretación, muchos ataques pueden pasar desapercibidos entre todo el ruido que genera el uso normal de la red.

3.6 Métodos de recolección de datos de los IDS

Existen determinados métodos, mediante los cuales, un IDS puede recabar información en nuestra red. Cada método tiene sus ventajas y desventajas, pero cada uno se ajusta mejor a un propósito determinado

3.6.1 Análisis de paquetes

Cualquier IDS que recolecta el tráfico que transita una red realiza análisis de paquetes.

Normalmente, la interfaz de un NIDS que debe recibir el tráfico a monitorizar se configura como *promiscua* para que capturen todo el tráfico que transita la red. Un NIDS no es capaz de recolectar el tráfico que transita la pila TCP/IP de un equipo, pero los HIDS sí son capaces de ver ese tráfico y analizarlo.

Hay diferentes maneras con las que un atacante puede intentar sobrepasar el análisis de paquetes de un IDS. Por ejemplo, pueden fragmentar los paquetes en paquetes más pequeños que no representen una amenaza a primera vista. Para evitar esto, los IDS implementan herramientas de agrupamiento de paquetes para su posterior análisis en conjunto.

3.6.2 Análisis de registros del sistema

Otro método muy utilizado por los IDS es analizar los ficheros de registros del sistema para encontrar registros que sean indicativos de una actividad anormal o sospechosa. Algunos ataques son altamente reconocibles por los registros que el sistema guarda en sus ficheros cuando se llevan a cabo.

3.6.3 Monitorización de llamadas al sistema

Los HIDS son capaces de instalarse dentro del núcleo del sistema para monitorizar las llamadas que los programas del equipo realizan a dicho núcleo, con el objetivo de detectar llamadas que supongan una actividad anormal o sospechosa. Por ejemplo, un HIDS puede detectar el intento de cambiar el identificador de un usuario para que coincida con el identificador del administrador con el fin de escalar los privilegios del usuario en cuestión.

3.6.4 Monitorización del sistema de ficheros

Un método muy común de recolección de datos de los HIDS es monitorizar los tamaños y atributos de ficheros cruciales de un sistema operativo. Por ejemplo, si el núcleo del sistema altera un archivo importante y ningún administrador es consciente de dicho cambio, podríamos estar ante un ataque.

3.7 Detección de intrusiones

Los IDS recolectan una cantidad de información muy amplia. Para que la detección de intrusiones sea efectiva entre tanta información, los IDS deben poseer algoritmos que determinen que tráfico merece la atención del administrador de la red.

Hay varias estrategias a escoger a la hora de identificar y clasificar el tráfico de red. Algunos administradores bloquean el tráfico malicioso, mientras que otros prefieren sólo permitir el que se sabe que es bueno. La primera estrategia se conoce como *Known Bad* (malo conocido) mientras que la segunda se conoce como *Known Good* (bueno conocido).

Si se adopta la estrategia de permitir sólo el tráfico bueno (Known Good), significa que se debe analizar todo el tráfico que transita la red con objetivo de marcar qué tráfico es normal y esperable en la red y que tráfico es extraño. Esto se traduce en una gran cantidad de información que el IDS debe analizar el tráfico y fragmentarlo para su posterior reconocimiento por parte del administrador. Además, el IDS se debe reajustar cada vez que la red cambia para reconsiderar qué es normal y qué es extraño. La ventaja de esta aproximación es que se pueden identificar más fácilmente ataques no conocidos, puesto que existen herramientas que, automáticamente, reconocen el comportamiento normal de una red y alertan ante cualquier cambio, sin necesidad de que un administrador interfiera demasiado.

Si se adopta la estrategia de bloquear sólo el tráfico malicioso (Known Bad), se traduce en una cantidad menor de avisos por parte del IDS, ya que el tráfico que se considera normal, transita de manera transparente para el administrador de la red. Debido a que las reglas de un IDS definen con exactitud que tráfico es malicioso, si se produce una alerta, eso significa que un ataque se está llevando a cabo sin ninguna duda. La desventaja de esto, es que un ataque que implique tráfico que las reglas del IDS no sepan reconocer pasará desapercibido. Si se implementan reglas más flexibles para ello, puede suponer un incremento de falsos positivos. Esta solución es más factible para administradores de red sin amplios conocimientos sobre seguridad, puesto que el surgimiento de una alerta no requiere mucha interpretación.

La elección de una estrategia u otra depende de las características y necesidades de cada red en particular. Si se quiere definir estrictamente el tráfico permitido, se debe elegir la estrategia de bueno conocido, mientras que, si se quiere ser más permisivo o la red cambia frecuentemente, una estrategia de malo conocido se ajusta mejor. En realidad, la mayoría de IDS combinan ambas estrategias.

3.8 Métodos de actuación ante la detección de un ataque

En lo referente a los métodos de actuación que los IDS pueden tomar a la hora de afrontar un ataque, ya sea una intrusión u otro tipo de ataque, tenemos varias aproximaciones.

3.8.1 Respuesta pasiva

Tradicionalmente, los IDS están configurados para generar reportes en ficheros y mandar alertas al administrador de red. Estas alertas pueden ser enviadas mediante trampas SNMP, un correo, mensajes al teléfono del administrador o incluso una llamada automatizada.

Lo normal es que un administrador configure el método de envío de una alerta que más se ajuste al nivel de importancia de la alerta. Por ejemplo, una alerta que sea generada por un falso positivo no debería ser notificada mediante llamadas de teléfono.

3.8.2 Respuesta activa

Los IDS también pueden ser configurados para que no sólo notifiquen al administrador de red ante una alerta, sino que también generen respuestas activas, es decir, que tomen medidas contra ese ataque para intentar detenerlo.

Los IDS pueden ser colocados en línea para que descarten tráfico que consideren malicioso, para que corten una conexión TCP enviando mensajes tanto al emisor como al

receptor, etc. También pueden enviar mensajes ICMP. Algunos IDS pueden reconfigurar un enrutador o un firewall para que el tráfico que se considera malicioso sea bloqueado.

3.8.3 IDS en línea

A la hora de implantar un IDS en una red, se puede instalar en un TAP en la red conmutada o puede instalarse en línea, es decir, entre los dispositivos finales e Internet. Cada aproximación tiene ventajas y desventajas en lo referente a la respuesta ante ataques.

Si se desea que un IDS genere respuestas activas ante un ataque, es más conveniente instalarlo en línea, puesto que es un dispositivo por el que transita el tráfico, porque si no se coloca en línea, el IDS puede influir en la detención de la comunicación entre dos dispositivos, pero no puede cortar el tráfico él mismo, depende de los dispositivos finales.

4 Análisis de vulnerabilidades

4.1 Introducción

Una vulnerabilidad es cualquier error de programación o de configuración que permite a un intruso obtener privilegios en un sistema. La mayoría de los equipos objetivo no son escogidos específicamente por un atacante, sino que pertenecen a una red cuyo espacio de direcciones es escaneado a fin de infectar a todos los equipos posibles dentro del mismo.

El análisis de vulnerabilidades es el proceso de encontrar e informar sobre las vulnerabilidades, ya sean de un equipo o de la red. Este análisis nos provee la oportunidad de solucionar las vulnerabilidades antes de que un intruso las pueda utilizar en su favor. Este análisis también ofrece la posibilidad de comprobar si las medidas de seguridad instaladas en una organización son efectivas. Por ejemplo, si hemos instalado un sistema IDS en la red, y al lanzar el análisis, no salta ninguna alerta en el IDS, el sistema no funciona correctamente.

Un análisis de vulnerabilidades puede tener varios propósitos. En la mayoría de las organizaciones en las que se analizan las vulnerabilidades, se utiliza un ciclo de análisis-reparación-verificación, es decir, se detecta una vulnerabilidad en un sistema, se repara, normalmente con la instalación de un parche, y se verifica que la reparación es correcta lanzando el análisis de nuevo. Otro uso común para el análisis de vulnerabilidades es la verificación de la seguridad de un sistema antes de ponerlo en producción, por ejemplo, un servidor web. Ante una crisis, un análisis de vulnerabilidades puede ser de gran ayuda, ya que ante un ataque, puede generar una lista de pasos a seguir que ayude al administrador de la red a paliar los efectos de la intrusión. Un análisis de vulnerabilidades también asiste al administrador de la red, ya que también es capaz de ofrecer un mapa general de la red: qué equipos hay, que recursos utilizan, que servicios se ofrecen, etc.

Uno de los usos más importantes de los análisis de vulnerabilidades es la correlación de los datos del análisis con las alertas generadas por un sistema IDS. Si se produce un ataque que genera una alerta por parte de un IDS, un reporte reciente de análisis de vulnerabilidades puede dar información sobre que vulnerabilidad en concreta explota el ataque, en que equipo se encuentra y que otros sistemas podrían haberse comprometido.

4.2 Tipos de análisis

A la hora de lanzar un análisis de vulnerabilidades en una organización, podemos analizar equipos en concreto, o analizar toda la red al mismo tiempo.

4.2.1 Análisis en equipos

El objetivo de este tipo de análisis de vulnerabilidades es detectar vulnerabilidades del sistema en el que reside el analizador, como permisos inseguros de ficheros, versiones de software desactualizadas, puertas traseras, troyanos, etc.

Este tipo de análisis requiere la instalación de paquetes de software y herramientas especializadas en cada sistema a analizar, así como privilegios de administrador. La profundidad del análisis en los equipos es lo que provoca que este tipo de análisis sea el preferido para sistemas críticos. El hecho de que la realización de un análisis sea costosa y la poca escalabilidad que conlleva la configuración individual de cada uno de los equipos, conlleva que este tipo de análisis se reserve para unos pocos sistemas críticos.

4.2.2 Análisis en red

El objetivo de este tipo de análisis es la detección de vulnerabilidades en cualquier sistema activo que esté conectado a la red en la cual se despliegue el analizador de vulnerabilidades.

Este tipo de análisis no requiere ningún tipo de configuración en los sistemas finales. La escalabilidad de este tipo de análisis es muy considerable, ya que, para añadir un sistema al mismo, sólo es necesario conectarlo a la red. Estas dos ventajas provocan que los análisis en red sean la única opción segura para analizar redes grandes y heterogéneas.

Los análisis en red también tienen algunas desventajas. Los análisis en red no son tan exhaustivos en los equipos como los análisis en equipo, lo que hace que los análisis en red no sean capaces de detectar ciertos tipos de vulnerabilidades. Los análisis en red pueden utilizar mucho ancho de banda de la red y crear grandes ficheros de reportes en los equipos que analizan.

4.3 Proceso de análisis de vulnerabilidades en red

Independientemente del producto que se utilice para llevar a cabo un análisis de vulnerabilidades en red, la mayoría seguirá el mismo proceso de análisis.

Detección de equipos activos

El administrador de red puede indicar que direcciones o que rangos de direcciones se deben analizar. El sistema detectará cuáles de las direcciones indicadas están asignadas a equipos activos en la red. La detección se realiza enviando mensajes ICMP o peticiones de conexiones TCP. Para aquellos equipos que solo aceptan comunicaciones con UDP, como servidores DNS externos o servidores RADIUS, muchos productos admiten la detección de equipos mediante mensajes UDP.

Identificación de equipos activos

Una vez que se han identificado los equipos activos en una red, se debe descubrir qué tipo de sistema reside en cada uno de dichos equipos activos. Los métodos utilizados para la

identificación van desde peticiones SNMP hasta identificaciones de sistemas que utilizan la pila de protocolos TCP/IP.

Enumeración de servicios

Cuándo los equipos activos de la red son localizados e identificados, el siguiente paso es un escaneo de los puertos de cada equipo para identificar que servicios ofrecen cada uno de ellos. Se realizan peticiones de conexiones TCP y UDP para comprobar que puertos abiertos tienen los equipos activos. Aunque hay 65.536 puertos disponibles en un equipo, lo normal es que se escanee un subconjunto de los mismos para reducir el congestionamiento de la red.

Identificación de servicios

Una vez que se listan los puertos que están activos en cada equipo, el siguiente paso es identificar el servicio que ofrecen cada uno de ellos. Para ello, se envían solicitudes de aplicaciones y se comparan las respuestas con firmas predefinidas.

Se pueden identificar servicios como HTTP en puertos diferentes del 80, servicios de correo como SMTP, POP3 e IMAP configurados con SSL, etc.

Identificación de aplicaciones

El siguiente paso es identificar las aplicaciones que están utilizando los servicios encontrados en el paso anterior, para determinar la organización que provee la aplicación que tipo de aplicación es, su versión, etc.

Esta información es útil porque el analizador de vulnerabilidades puede encontrarse con varios problemas. Puede que un test de vulnerabilidades específico cause el fallo de la aplicación que está analizando. Si se conoce la aplicación previamente, se puede evitar lanzar dicho test.

Los falsos positivos son un gran problema de los análisis de vulnerabilidades. Si no se tiene información de las aplicaciones o está incompleta, se puede registrar un falso positivo debido a que los desarrolladores de los test asumieron que la aplicación vulnerable siempre residiría en el equipo activo. Una aplicación diferente puede responder al test de manera que el analizador lo interprete como un positivo. Si se tiene información sobre las aplicaciones sobre las cuales se ejecutan los test, se pueden evitar los falsos positivos.

Identificación de vulnerabilidades

Tras identificar las aplicaciones que utilizan los servicios detectados, se debe comenzar el proceso de detección de vulnerabilidades.

El analizador debe detectar las vulnerabilidades sin provocar efectos laterales como provocar el fallo del equipo o la aplicación que está analizando. Normalmente, el analizador detectará la vulnerabilidad, pero no la explotará por completo.

Informe de vulnerabilidades

Una vez que el análisis de vulnerabilidades ha finalizado, el sistema debe informar al administrador de red sobre que vulnerabilidades ha encontrado y en qué equipos de la red residen.

4.4 Perspectivas en el análisis de vulnerabilidades

A la hora de automatizar un análisis de vulnerabilidades, la perspectiva que toma el analizador es esencial para que el análisis asegure la mayor eficacia en el resultado.

4.4.1 Perspectiva de administrador

La perspectiva de administrador es utilizada por el analizador para realizar el análisis desde el punto de vista de un usuario administrador con privilegios. La herramienta de análisis debe ser lanzada por un usuario administrador o con las credenciales necesarias. El analizador puede detectar qué parches faltan en los equipos, configuraciones inseguras, y software vulnerable en el lado del cliente.

Esta perspectiva es útil para redes cuyos equipos activos son en mayoría sistemas Windows que se autentican en un servidor remoto. Los analizadores tienen pocas probabilidades de influir negativamente en el proceso normal de los equipos activos que analizan, por lo que los análisis pueden llevarse acabo en las horas de producción de la organización.

La perspectiva de administrador es útil para detectar vulnerabilidades en las aplicaciones cliente en los equipos finales de una red, ya que la mayoría de software malicioso explota vulnerabilidades en clientes de e-mail y navegadores web.

Esta perspectiva también tiene limitaciones. Cualquier sistema que utilice un medio diferente de autenticación (dominio diferente, servidor diferente, etc.), no serán analizados. Los firewalls también influyen negativamente en el correcto devenir del análisis de vulnerabilidades hacia dispositivos en subredes diferentes, como zonas desmilitarizadas.

4.4.2 Perspectiva del atacante externo

Las herramientas de análisis que usan esta perspectiva toman el papel de un atacante externo sin autorización para entrar en los sistemas. La ventaja de esta perspectiva es la posibilidad de analizar un rango de sistemas operativos y servicios más amplio de la perspectiva de administrador.

El objetivo es que la herramienta de análisis ofrezca al administrador de red los mismos resultados que un atacante externo obtendría en el caso de que realizara un escaneo de la red. Esta perspectiva provee de información de ataques comunes, a diferencia de la perspectiva de administrador que se centra en parches y malas configuraciones. En resumen, esta perspectiva ofrece una lista de ataques posibles que un atacante externo podría llevar a cabo.

Esta perspectiva tiene desventajas. Muchas de las vulnerabilidades existentes en una aplicación no pueden ser analizadas sin provocar el fallo de la aplicación o del equipo en el que reside. Normalmente, las herramientas ofrecen una opción de "análisis intrusivo" para tratar con éste tipo de vulnerabilidades.

4.4.3 Perspectiva híbrida

Las herramientas que utilizan esta perspectiva utilizan la perspectiva de administrador cuando poseen las credenciales necesarias y la autenticación es posible, y en el caso de que no sea posible, utilizan la perspectiva del atacante externo para llevar a cabo el análisis de vulnerabilidades.

Una de las grandes ventajas de la utilización de esta perspectiva es que las herramientas pueden identificar la existencia de una vulnerabilidad, independientemente de si un parche ha sido aplicado o no en el sistema. Por ejemplo, un parche que soluciona una vulnerabilidad concreta ha sido instalado, pero no afecta al sistema hasta que se éste se reinicia, pero al administrador del equipo se le olvida reiniciar el sistema, por lo que sigue siendo vulnerable. Una herramienta que sigue la perspectiva de administrador determinaría que ese sistema es seguro, pero una herramienta que sigue la perspectiva de atacante externo detectaría el fallo en el sistema.

4.5 Limitaciones del análisis de vulnerabilidades

Las herramientas de análisis no sustituyen una auditoría de seguridad manual, puesto que muchas de las vulnerabilidades más comunes son indetectables.

Por ejemplo, muchas aplicaciones web son desarrolladas en periodos de tiempo muy reducidos o bajo requerimientos de usuario poco seguros. Esto puede provocar que la aplicación no realice comprobaciones de seguridad sobre entradas del usuario. Esta falta de comprobaciones de seguridad siempre es detectada más rápido por un experto en seguridad que por una herramienta de análisis de vulnerabilidades automatizada.

5 Sistema de Información de Seguridad y Administración de Eventos

Un Sistema de Información de Seguridad y Administración de Eventos (SIEM) es un sistema utilizado en redes de datos para el análisis en tiempo real de eventos e información de seguridad, como alertas generadas por hardware de red, aplicaciones, acciones de usuarios, etc.

Los SIEMs se componen dos secciones principales: Información de seguridad y administración de eventos.

- **Información de seguridad**. Esta sección provee de almacenamiento de larga duración, manipulación y reportes de datos adquiridos por la sección de administración de eventos.
- **Administración de eventos**. Esta sección se encarga de la monitorización en tiempo real, de la correlación de eventos, de las notificaciones, etc.

Uno de los objetivos principales de los SIEMs es monitorizar y ayudar en la gestión de los activos de la red, de los usuarios y de todos los aspectos de una empresa relacionados con su red de datos.

La mayoría de SIEMs funcionan desplegando un conjunto de agentes recolectores, o sensores, de manera jerárquica, cuya función es recoger información de dispositivos de usuarios, servidores, equipos de red, cortafuegos, antivirus, IPS, etc. Ese conjunto de agentes recolectores envía la información recogida a una consola de administración central que realiza inspecciones y marca las anomalías para su posterior análisis en profundidad por parte de un especialista.

Las características principales de los SIEMs son las siguientes:

- **Agregación de datos** desde diferentes fuentes.
- **Correlación de eventos** diferentes a través de características comunes o patrones de comportamiento que llevan a descubrir eventos de seguridad más avanzados.
- **Alertas** instantáneas sobre aquellos eventos de seguridad que más prioridad tienen y que suponen un mayor peligro para la organización.
- **Paneles de información** sobre estadísticas de los eventos y la información de seguridad recolectada en la red.
- **Información para cumplimiento de auditorías.**
- **Retención** de datos a largo plazo para cumplir con los requerimientos de las auditorías y para permitir análisis forense en un mayor rango de tiempo.
- **Análisis forense** mediante búsquedas avanzadas en todos los logs generados por el sistema.

Dos de los componentes principales que conforman el software que un SIEM contiene para llevar a cabo toda su funcionalidad de monitorización, recolección y alertas son:

- Detección de intrusiones (IDS), tanto en red (NIDS) como en host (HIDS).
- Escáner de vulnerabilidades.

Dichos componentes poseen las características indicadas en los apartados anteriores correspondientes del estudio teórico y son totalmente configurables desde la consola centralizada del SIEM .

Algunos ejemplos de herramientas SIEM disponibles en el mercado son las siguientes:

- **ArcSight ESM**: SIEM desarrollado por ArcSight, propiedad de HP Enterprise. Este SIEM tiene licencia de pago y tiene varias versiones. Dependiendo de la versión a la que de acceso la licencia, la capacidad de procesado de datos del sistema varía desde 20 GB por día hasta 250 GB por día. Las ventajas de este SIEM son su adaptabilidad al tamaño de la empresa mediante las versiones del sistema y la conexión con la comunidad para la constante retroalimentación sobre peligros emergentes. Como desventaja, este SIEM ofrece un pobre sistema de análisis forense.
- **EMC RSA Security Analytics**: SIEM desarrollado por RSA, una filial de EMC, propiedad de DELL. Este SIEM es modular y su adquisición puede adaptarse según los módulos que más interés tengan para cada organización. Como ventaja, este SIEM tiene la capacidad de adaptarse a las necesidades más concretas de cada organización debido a su arquitectura modular. Como desventaja, este SIEM puede no ser rentable para pequeñas organizaciones que desean poseer toda la

información de seguridad, para lo que es necesario adquirir el software completo y puede conllevar altos gastos en recursos, tanto dinero, hardware y software.

- **Solarwinds Log and Event Manager**: SIEM desarrollado por SolarWinds. Este SIEM privativo está disponible como una solución para entornos virtualizados VMWare ESX y Microsoft Hyper-V. Según la versión de la solución que se adquiera, la cantidad de nodos que puede monitorizar varía desde 30 hasta 2500. Como ventajas de este SIEM, tenemos la característica de que es un SIEM para entornos virtualizados, lo que conlleva todas las ventajas de dicho tipo de entornos. La desventaja de este SIEM es, que si una empresa no dispone de un entorno virtualizado sobre el que desplegar el SIEM, no puede implantarlo en su red corporativa.
- **Alienvault OSSIM**: SIEM gratuito desarrollado por Alienvault. Ofrece todas las características de un SIEM tradicional con la ventaja de que es un software de código abierto y se puede modificar para ajustarse a las necesidades de cada organización. OSSIM no tiene límites de nodos que monitorizar ni límite de procesado de datos bajo licencia privativa. Los límites de nodos, procesado de datos, etc., están limitados por el hardware sobre el que se despliega OSSIM, por lo que la escalabilidad del SIEM es directamente proporcional a las capacidades de dicho hardware. Para ofrecer todas las funcionalidades de un sistema SIEM, OSSIM agrupa un amplio conjunto de herramientas gratuitas de código abierto:
    - PRADS, para la identificación pasiva de activos y servicios.
    - OpenVAS, para análisis de vulnerabilidades.
    - Suricata, para la detección de intrusos en red (NIDS).
    - OSSEC, para la detección de intrusos en host (HIDS).
    - NFSen, para la generación de estadísticas de uso de la red.

  OSSIM también ofrece aplicaciones de terceros, como por ejemplo, un motor de correlación genérico. También ofrece la posibilidad de recolectar logs de equipos de otros fabricantes, como cortafuegos, equipos de red, etc. Aunque OSSIM ofrece todas las capacidades SIEM de manera gratuita, Alienvault ofrece dos versiones de su SIEM para entornos virtualizados con licencia de pago: USM Appliance y USM Anywhere.

La mayor ventaja de OSSIM, a parte de su licencia GPL, es la conexión directa que tiene con OTX (Open Threat Exchange). OTX es una comunidad abierta de Alienvault para el intercambio constante de peligros emergentes donde se pueden encotrar IPs maliciosas, URLs maliciosas e incluso patrones de ataque. Toda esta información es utilizada por OSSIM en su motor de correlación para analizar los eventos que se generan en la red de una organización. La desventaja de OSSIM es que es la primera versión de los SIEMs de Alienvault en recibir las actualizaciones, por lo que a veces, dichas actualizaciones pueden ser inestables. Esta desventaja se suple de manera bastante eficiente con un foro para contactar directamente con los desarrolladores de OSSIM y recibir atención personalizada sobre diferentes problemas y/o incidencias.

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

REF: 0000001

ANEXO A: SEDES REMOTAS DE EPICSA

CLIENTE: EMPRESA PROVINCIAL DE INFORMACIÓN DE CÁDIZ S.A. (EPICSA)
PLAZA MADRID S/N, EDIFICIO CARRANZA, FONDO SUR, LOCAL 10, 11010 CÁDIZ
956261500

AUTOR: CARLOS CARRETERO AGUILAR
INGENIERO INFORMÁTICO
25603515-F
CARLOS.CARRETEROAGUILAR@ALUM.UCA.ES

FIRMADO:
SOLICITANTE AUTOR

CÁDIZ, A 1 DE JULIO DE 2017

1 Centros externos

CENTRO	DOMICILIO
Servicio Provincial de Recaudación y Gestión Tributaria	
ARGISA Mancomunidad del Campo de Gibraltar	Autovía A7, Salida 113 11370 Los Barrios
PIT – Valdelagrana	Paseo Marítimo nº 11, Urbanización Valdemar, Bl8, B-dcha 11500 El Puerto de Santa María
PIT - El Juncal	Avda. de la Música nº 2, local 12 11500 El Puerto de Santa María
PIT – Rio San Pedro	Avda. de la Bahía nº 12 11519 Puerto Real
SPR Alcalá de los Gazules	Alameda de la Cruz s/n 11180 Alcalá de los Gazules
SPR Alcalá del Valle	Calle Real s/n 11693 Alcalá del Valle
SPR Algar	C/La Fuente nº7 11639 Algar
SPR Algeciras	Avda. Capitán Ontañón, Ed.Ç Mª Cristina local 2 11202 Algeciras
SPR Inspección Algeciras	Calle Lola Peche nº 1 Bajo 11201 Algeciras
SPR Algodonales	Avda. Constitución nº 44 11680 Algodonales
SPR Arcos de la Frontera	C/12 de Octubre nº 2 11630 Arcos de la Frontera
SPR Barbate	C/Camilo José Cela nº 8 11160 Barbate
SPR Benalup	C/Canteras s/n 11190 Benalup
SPR Bornos	Plaza Alcalde José González nº 2, Patio interior del Castillo 11640 Bornos
SPR Chipiona	C/ Miguel de Cervantes nº 36 11550 Chipiona
SPR Conil de la Frontera	C/Federico García Lorca nº 5, Bajo

CENTRO	DOMICILIO
	11140 Conil de la Frontera
SPR Espera	Bajo del Ayuntamiento, C/Andalucía nº 11 11648 Espera
SPR Jerez de la Frontera	C/ Francisco Riba nº6, Ed. Forum Chapin, locales 1-9 11405 Jerez de la Frontera
SPR Jimena de la Frontera	C/ Sevilla, Casa de la Cultura 11330 Jimena de la Frontera
SPR Los Barrios	Urb. El Lazareto, C/ la Esparraguera 11370 Los Barrios
SPR La Línea de la Concepción	Calle Real nº 1, esquina con Pl. de la Constitución 11300 La Línea de la Concepción
SPR Medina Sidonia	Avda. Andalucía nº 25 11170 Medina Sidonia
SPR Olvera	C/ Bellavista nº 16 11690 Olvera
SPR Paterna de Rivera	C/Peteneras nº 14, Bajo 11178 Paterna de Rivera
SPR Prado del Rey	C/Doctor González Quevedo nº 7 11660 Prado del Rey
SPR Puerto Real	Paseo Marítimo nº 2 11510 Puerto Real
SPR Puerto Serrano	Avda. de las Escuelas nº 5 11659 Puerto Serrano
SPR El Puerto de Santa María	C/Larga nº 39 11500 El Puerto de Santa María
SPR Rota	C/Ubrique nº 1 11520 Rota
SPR San Fernando	C/Montigny nº 7 11100 San Fernando
SPR San José del Valle	Plaza de Andalucía nº 15 11580 San José del Valle
SPR Sanlúcar de Barrameda	C/ Banda playa nº 45, Edificio ERESSAN 11540 Sanlúcar de Barrameda
SPR San Martín del Tesorillo	c/Tufas

CENTRO	DOMICILIO
	11340 San Martín del Tesorillo
SPR San Roque	C/San Felipe nº 7 11360 San Roque
SPR Tarifa	C/ Batalla del Salado nº 24 11358 Tarifa
SPR Trebujena	C/ Veracruz nº 4 11560 Trebujena
SPR Ubrique	C/ Juzgado Nº 3 Ed. SS Múltiples 1ª y 4ª Planta 11600 Ubrique
SPR Unidad Técnica de Sanciones	Avda. de la Ilustración nº 6, Ed. Astarté, 1º Planta Local 9 11010 Cádiz
SPR Vejer de la Frontera	Plaza de Juan Bueno nº 4 11150 Vejer de la Frontera
SPR Villamartín	C/ Extramuros nº 131 11650 Villamartín
Otros Centros	
Fundación Medio Ambiente, Energía y Sostenibilidad de la Provincia de Cádiz	Avenida del Puerto, nº1. Ed. Trocadero, 1º. C1-C2 11006 Cádiz
Consorcio Bahía de Cádiz	Av, Ramón de Carranza, 18 – 3ª Planta 11006 Cádiz
SAM Jimena de la Frontera	C/ Sevilla, 79 11330 Jimena de la Frontera
SAM Medina Sidonia	C/ Nuestra Señora de la Salud, 1 11170 Medina Sidonia
SAM Olvera	C/ Vereda Ancha, 34 11690 Olvera
SAM Villamartín	Alameda de Diputación, s/n 11650 Villamartín
Residencia Provincial de El Puerto de Santa María	C/ Zarza 3 11500 El Puerto de Sta. María
Residencia Provincial de la Línea de la Concepción	C/ Doctor Gómez Ulla s/n 11300 La Linea de la Concepción
Centro de Educación Ambiental El	Barriada de la Feria, s/n.

CENTRO	DOMICILIO
Castillejo	11670 El Bosque
Centro Agrícola Ganadero	Ctra. Jerez-Arcos, S/n 11592 Torre Melgarejo
IFECA	Parque González Hontoria, s/n 11405 Jerez de la Frontera
Parque Móvil	Vía de Italia, s/n - Recinto Interior Zona Franca 11011 Cádiz

Tabla 24 Lista de centros externos con conexión VPN IP/Macrolan

2 Ayuntamientos

POBLACIÓN	DOMICILIO
Alcalá de los Gazules	Alameda de la cruz, 13 11180 Alcalá de los Gazules
Alcalá del Valle	Plaza del ayuntamiento,1 11693 Alcalá del Valle
Algar	Plaza de la Constitución,1 11639 Algar
Algeciras	Alfonso XI, 12 11201 Algeciras
Algodonales	Avda. Andalucía, 2 11680 Algodonales
Barbate	Plaza de la Inmaculada, s/n 11160 Barbate
Benalup-Casas Viejas	c/ Cantera, s/n 11190 Benalup-Casas Viejas
Benamahoma	c/ Real, 42 11679 Benamahoma
Benaocaz	Plaza de las libertades, 1 11612 Benaocaz
Bornos	Plaza Alcalde José González, 1 11640 Bornos
Castellar de la Frontera	Plaza de Andalucía s/n 11350 Castellar de la Frontera

POBLACIÓN	DOMICILIO
Chidana de la Frontera	c/ de la Constitución, 1 11130 Chidana de la Frontera
Chipiona	Plaza Andalucía s/n 11550 Chipiona
Conil de la Frontera	Plaza de la Constitución, 1 11140 Conil de la Frontera
El Bosque	Pza. de la Constitución, 2 11670 El Bosque
El Gastor	Pza. de la Constitución, 12 y 14 11687 El Gastor
El Puerto de Santa María - Serecop	Virgen De Los Milagros, 59 11500 El Puerto de Santa María
Espera	c/ Andalucía, 31 11648 Espera
Grazalema	Plaza de España, 1 11610 Grazalema
Jerez de la Frontera- JESSYTEL	C/ Larga, 32 11402 Jerez de la Frontera
Jimena de la Frontera	c/ Sevilla, 61 11330 Jimena de la Frontera
E.L.A. La Barca de la Florida	Plaza del Ayuntamiento, 1 11570 La Barca de la Florida
La Línea de la Concepción	Pza. García Cabreros, s/n 11300 La Línea de la Concepción
Los Barrios	Plaza de la iglesia, 1 11370 Los Barrios
Medina Sidonia	Plaza de España, 1 11170 Medina Sidonia
Olvera	Plaza del Ayuntamiento, 1 11690 Olvera
Paterna de Rivera	Plaza de la Constitución, 1 11178 Paterna de Rivera
Prado del Rey	Pza. Constitución, 1 11660 Prado del Rey

POBLACIÓN	DOMICILIO
Puerto Serrano	Pza. de Miguel Rodríguez Rivera, s/n 11659 Puerto Serrano
Rota	c/ Cuna 2 11520 Rota
San José del Valle	Plaza de Andalucía, 15 11580 San José del Valle
Sanlúcar de Barrameda	Palacio Municipal. Cuesta de Belén s/n 11540 Sanlúcar de Barrameda
San Fernando	C/ Real, 185 11100 San Fernando
E.L.A. San Martín del Tesorillo	c/Tufas 11340 San Martín del Tesorillo
San Roque	Plaza de Armas, 13 11360 San Roque
Setenil de las Bodegas	c/ Villa, 5 11692 Setenil de las Bodegas
Tarifa	Plaza de Santa María, 3 11380 Tarifa
Torre Alháquime	Plaza de la Constitución, 1 11691 Torre Alháquime
Trebujena	Plaza de España, 1 11560 Trebujena
Ubrique	La Plaza, 1 11600 Ubrique
Vejer de la Frontera	Plaza de España, 1 11150 Vejer de la Frontera
Villaluenga del Rosario	c/ Real, 19 11611 Villaluenga del Rosario
Villamartín	Plaza del Ayuntamiento, 1 11650 Villamartín
Zahara de la Sierra	Plaza del Rey, 1 11688 Zahara de la Sierra
E.L.A. Zahara de los Atunes	Drs. Sánchez Rodríguez, S/N 11393 Zahara de los Atunes

Tabla 25 Lista de ayuntamientos con conexión VPN IP/Macrolan

3 Otras oficinas

SEDE	DOMICILIO
Oficinas del Servicio de Drogodependencias	
Equipo de tratamiento de Algeciras	
CTA Algeciras	C/ Miguel Hernández, 17 Bda. El Saladillo 11207 Algeciras
Equipo de Apoyo en II.PP. Algeciras-Botafuegos	Carretera del Cobre, Km. 45 11206 Algeciras
Equipo de tratamiento de Chiclana	
CTA Chidana de la Frontera	C/ Plaza de la Soledad, 1 11130 Chidana de la Frontera
Equipo de tratamiento de La Janda	
CTA Alcalá de los Gazules	C/ Miguel Tizón, 5 11180 Alcalá de los Gazules
CTA Barbate	Avenida del Rio, 42 11160 Barbate
CTA Conil de la Frontera	Plaza Santa Catalina, S/N 11140 Conil de la Frontera
Equipo de tratamiento de Jerez	
CTA Jerez de la Frontera	C/ Vicario, 18 11403 Jerez de la Frontera
Equipo de Apoyo en II.PP. Puerto I y Puerto II	Carretera Jerez-Rota, s/n 11500 El Puerto de Santa María
Equipo de tratamiento de La Línea de la Concepción	
CTA La Línea de la Concepción	C/ Xauen, s/n 11300 La Línea de la Concepción
Equipo de tratamiento Bahía de Cádiz	
CTA Puerto Real	C/ San Alejandro, 2 11510 Puerto Real
CTA San Fernando	Avda. Cornelio Balbo, s/n (B. Blas Infante) 11100 San Fernando
Equipo de tratamiento de Sanlúcar de Barrameda	
CTA Sanlúcar de Barrameda	C/ Puerto, s/n

SEDE	DOMICILIO
	11540 Sanlúcar de Barrameda
Equipo de tratamiento Sierra Norte	
CTA Algodonales	C/ Arcos, 29 (bajo) 11680 Algodonales
CTA Ubrique	C/ Ingeniero Romero Carrasco, nº 28 11600 Ubrique
Equipo de tratamiento Sierra Sur	
CTA Arcos de la Frontera	C/ Nueva, s/n 11630 Arcos de la Frontera
CTA Villamartín	C/ Ebro, s/n 11650 Villamartín
Equipo de tratamiento de El Puerto de Santa María	
CTA El Puerto de Santa María	Plaza del Castillo, 7 11500 El Puerto de Santa María
Equipo de tratamiento de Rota	
CTA Rota	Plaza Camilo José Cela, 1 11520 Rota

Tabla 26 Lista de otras oficinas con conexión VPN IP/Macrolan

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

REF: 0000001

ANEXO B: ENTREVISTA CON EPICSA

CLIENTE: EMPRESA PROVINCIAL DE INFORMACIÓN DE CÁDIZ S.A. (EPICSA)
PLAZA MADRID S/N, EDIFICIO CARRANZA, FONDO SUR, LOCAL 10, 11010 CÁDIZ
956261500

AUTOR: CARLOS CARRETERO AGUILAR
INGENIERO INFORMÁTICO
25603515-F
CARLOS.CARRETEROAGUILAR@ALUM.UCA.ES

FIRMADO:
SOLICITANTE AUTOR

CÁDIZ, A 1 DE JULIO DE 2017

1 Entrevista con EPICSA

El objetivo de la entrevista que se realiza con el cliente del presente proyecto es recabar la máxima información posible sobre:

- Estado actual de la red corporativa.
- Procedimientos de administración de red.
- Estado actual de la gestión de información de seguridad en la empresa.
- Sistemas de monitorización instalados.
- Necesidades de recabado de diferentes tipos de datos.
- Niveles de importancia de los activos de la empresa.
- Número de usuarios encargados de la administración de la red corporativa.
- Necesidades sobre almacenamiento de los resultados de la monitorización.

A continuación, se expone un extracto de la entrevista con Manuel Añón Rodríguez, coordinador del departamento de redes y telecomunicaciones de la Empresa Provincial de Información de Cádiz S.A. (EPICSA).

Tras los saludos y presentaciones iniciales pertinentes, pasamos al núcleo de la entrevista.

P: Sería necesario que me explicara de manera general en qué estado global se encuentra su red corporativa.

R: En EPICSA administramos la red corporativa de la Diputación Provincial de Cádiz, que interconecta todas las sedes provinciales de la Diputación y todos los ayuntamientos de la Provincia de Cádiz con menos de 20.000 habitantes. En nuestra empresa, tenemos desplegada una zona desmilitarizada para la provisión de servicios al público y un centro de datos para la prestación de servicios a todos los empleados de la Diputación.

P: ¿Dispondría de alguna documentación técnica completa sobre la red corporativa que ustedes administran?

R: Por supuesto, disponemos de la documentación técnica que Telefónica desarrolló durante la realización del proyecto de construcción de nuestra red corporativa.

P: Hablando del proceso de administración de la red que ustedes realizan diariamente, ¿qué herramientas utilizan para apoyar su labor?

R: Actualmente disponemos de un sistema de monitorización de servicios implementado con la herramienta Zabbix que nos avisa automáticamente cuándo ocurre alguna incidencia con, algún dispositivo de red, ya sea una congestión de recursos, un corte de electricidad, un apagado, etc.

Para la configuración de los dispositivos mezclamos la configuración mediante interfaces web y consola.

P: En cuanto a los aspectos de seguridad, ¿qué puede decirme de la red que ustedes administran?

R: Disponemos de una serie de firewalls desplegados en la red para controlar los accesos a diferentes puntos de la red. Para monitorizar los ataques externos que nuestra red pudiera sufrir, el Centro Criptográfico Nacional ha desplegado un sensor en la zona frontera de nuestra red. El problema que tenemos es que ese sensor no lo administramos nosotros y estamos totalmente desprotegidos ante ataques internos. Tampoco disponemos de ningún sistema que analice y alerte sobre las vulnerabilidades presentes en los activos de nuestra empresa.

Para proteger los ordenadores con sistema operativo Windows, tenemos instalado en todos ellos un antivirus, pero no disponemos de un sistema centralizado que nos alerte sobre si ha entrado un virus en un ordenador, si alguien intenta entrar en un ordenador, etc.

P: Entiendo entonces que necesitan algún sistema que monitorice las áreas internas de su red corporativa.

R: Efectivamente. Lo ideal sería disponer de un sistema que monitorizara todo el tráfico que transita nuestra red, especialmente la zona frontera, pues es la zona que tenemos abierta al público.

P: Hoy en día existen muchas herramientas que integran más aspectos de la monitorización de red, incluyendo los aspectos de seguridad. ¿Qué tipo de información sería útil que les proporcionara el sistema de monitorización de la red interna?

R: Incluyendo los aspectos meramente de seguridad de la información, hay que tener en cuenta que nuestra red es bastante grande, por lo que toda la información que el sistema nos pueda dar nos sería muy útil, por ejemplo, inventario de todos los activos de la red y estadísticas de uso de la red.

P: Normalmente, a la hora de desplegar un sistema de monitorización de red, es interesante definir qué activos de su red son más valiosos que otros. ¿Qué puede decirme sobre esto?

R: Nuestros activos más importantes son los que se encuentran en la zona desmilitarizada, puesto que son los activos que prestan servicio al público. En el mismo nivel, también son igual de importantes todos los cortafuegos desplegados en nuestra red. En un segundo nivel, todos los servidores que tenemos en el centro de datos también son muy importantes, haciendo hincapié en aquellos servidores que se conectan con algunos equipos de la DMZ para proporcionar ciertos recursos. El resto de activos, en un tercer nivel, son igual de importantes.

P: ¿Cuántos usuarios serían los encargados de utilizar la herramienta?

R: En nuestra empresa somos dos técnicos de redes en total, así que ese sería el número de usuarios totales del sistema. Los dos usuarios deben tener privilegios de administrador en la herramienta.

P: ¿Qué otras consideraciones debería tener en cuenta sobre su red a la hora de diseñar el sistema de monitorización?

R: La Diputación de Cádiz es una Administración pública, y como tal, debe adaptarse a las directrices desarrolladas en el Esquema Nacional de Seguridad, así que el sistema de monitorización debe cumplir también dichas directrices:

- Almacenamiento de los registros durante, como mínimo, dos años.
- Sistemas de copias de seguridad para restablecimiento de los registros.

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

REF: 0000001

ANEXO C: INSTALACIÓN DEL SIEM

CLIENTE: EMPRESA PROVINCIAL DE INFORMACIÓN DE CÁDIZ S.A. (EPICSA)
PLAZA MADRID S/N, EDIFICIO CARRANZA, FONDO SUR, LOCAL 10, 11010 CÁDIZ
956261500

AUTOR: CARLOS CARRETERO AGUILAR
INGENIERO INFORMÁTICO
25603515-F
CARLOS.CARRETEROAGUILAR@ALUM.UCA.ES

FIRMADO:
SOLICITANTE AUTOR

CÁDIZ, A 1 DE JULIO DE 2017

1 Instalación del sistema operativo

Todas las instalaciones de OSSIM, tanto el servidor como los sensores, son instalaciones del sistema operativo GNU/Linux Debian con una selección de software determinada, a parte del sistema operativo base.

Para instalar OSSIM, la empresa nos ofrece una imagen .ISO con todo lo necesario para instalar el SIEM. Cuando arrancamos la instalación desde un CD o USB, lo primero que vemos es que nos da a elegir qué tipo de instalación vamos a hacer: servidor o sensor. El proceso de instalación del sistema operativo es igual para los dos perfiles, simplemente que, dependiendo del perfil elegido, se instalará automáticamente un conjunto de software predefinido u otro.

Figura 114 Instalación OSSIM - Pantalla inicial

A partir de ahora, todos los pasos a seguir serán iguales tanto para el servidor como para los sensores, hasta que lleguemos a la configuración después de instalar el sistema operativo base.

Lo primero que tenemos que hacer es escoger el idioma de la instalación y la ubicación geográfica, que, en este caso, serán español y España, respectivamente.

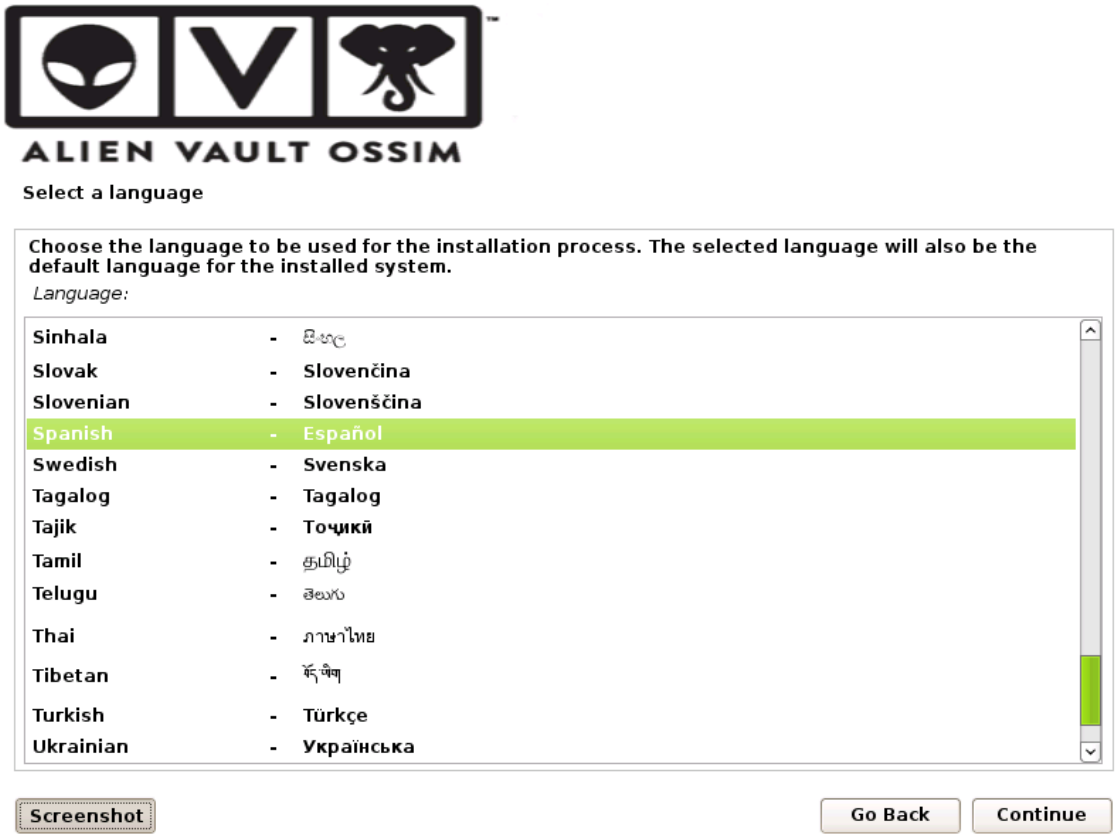


Figura 115 Instalación OSSIM - Selección idioma

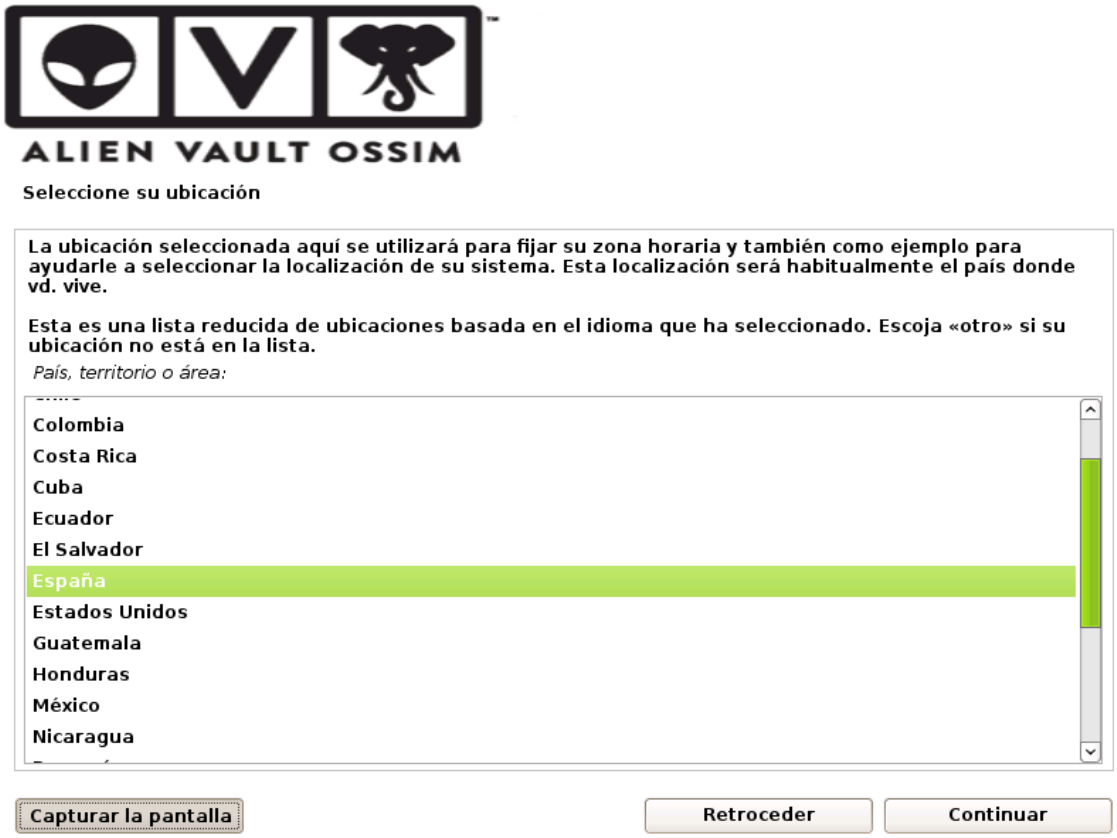


Figura 116 Instalación OSSIM - Selección ubicación geográfica

Seguidamente, hay que indicar la configuración de teclado que disponemos, que, en este caso, será español.

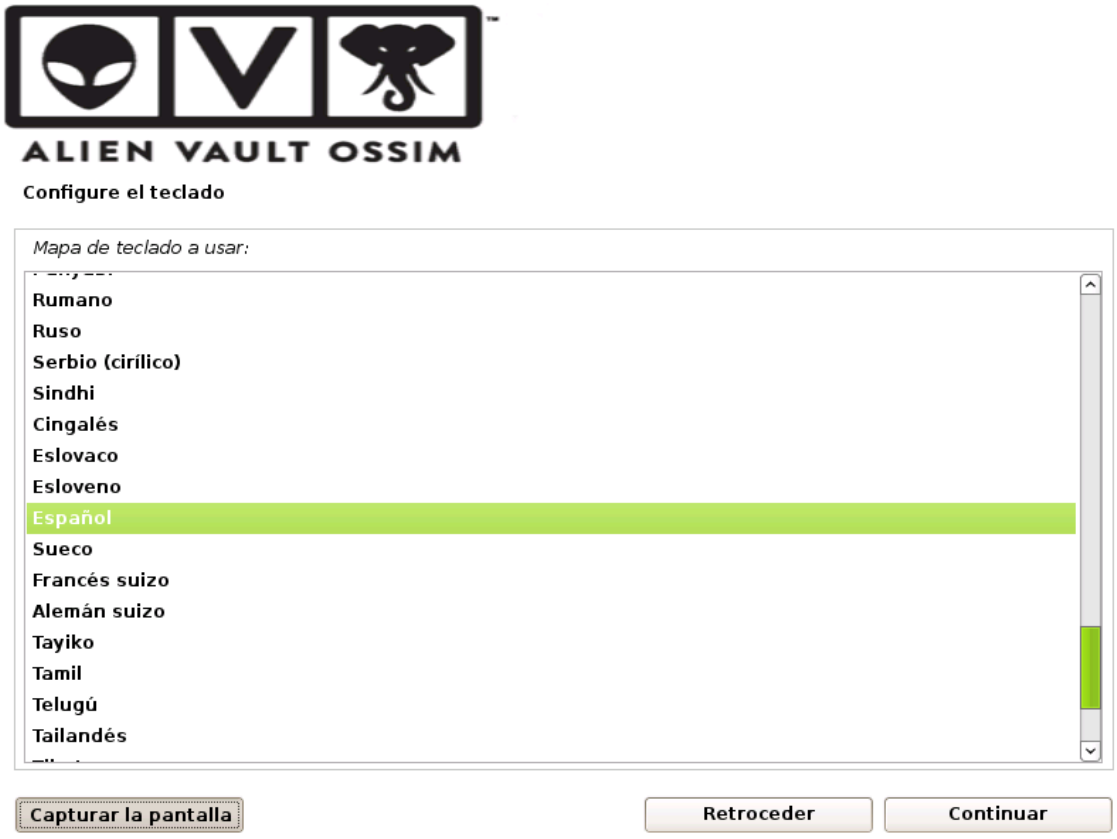


Figura 117 Instalación OSSIM - Selección de distribución de teclado

Tras cargar los componentes del instalador del CD o del USB en el que tengamos instalada la imagen del sistema OSSIM, debemos elegir la interfaz de red primaria que, tanto para el servidor como para los sensores, será la interfaz de administración.

Figura 118 Instalación OSSIM - Selección interfaz administración

A continuación debemos configurar la dirección IP de dicha interfaz primaria, su máscara de subred, la dirección IP de la puerta de enlace y la dirección IP del servidor de nombres de dominio.

Figura 119 Instalación OSSIM - Configuración dirección IP

Figura 120 Instalación OSSIM - Configuración de máscara de subred

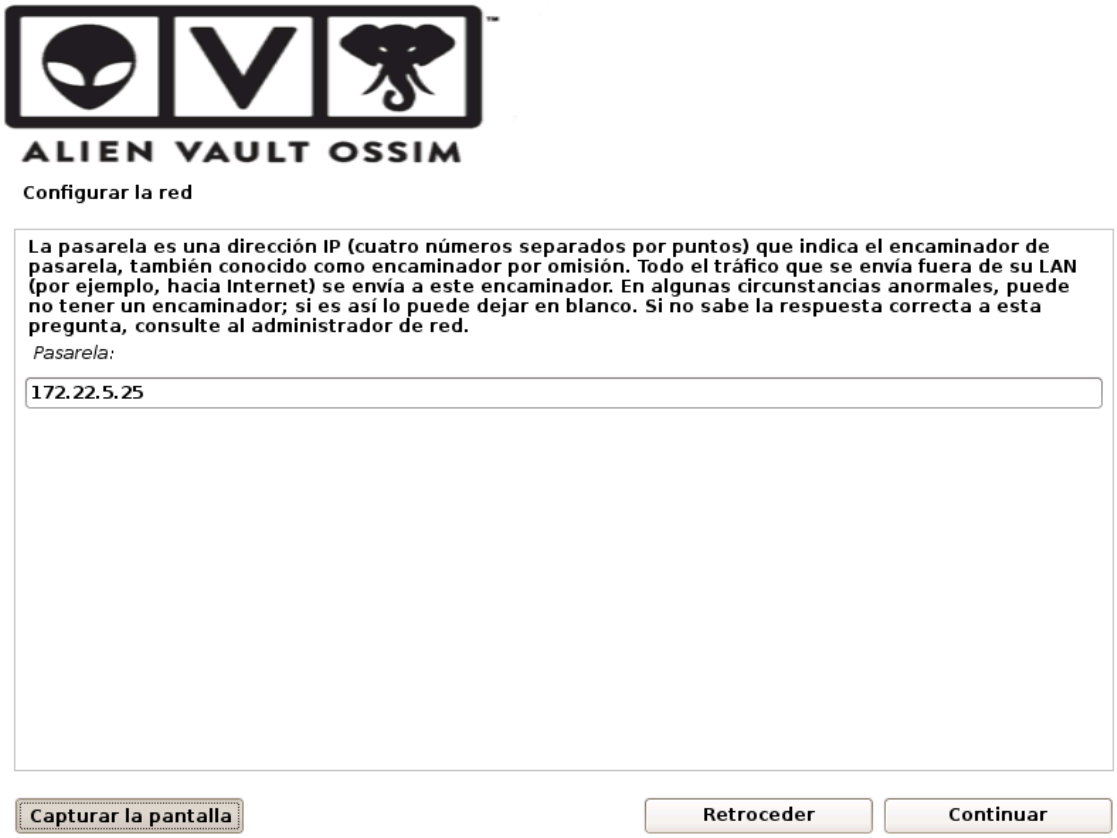


Figura 121 Instalación OSSIM - Configuración de dirección de la puerta de enlace

Figura 122 Instalación OSSIM - Configuración de DNS

A continuación, debemos configurar la contraseña del súper usuario "root", que será el único usuario existente en el sistema desde el que podamos acceder al servidor/sensor o, al menos, así es por defecto.

Figura 123 Instalación OSSIM - Configuración contraseña del usuario root

Por último, debemos elegir la zona horaria del servidor/sensor que, en este caso, será la Península.

Figura 124 Instalación OSSIM - Configuración de la zona horaria

A partir de ahora y, automáticamente, el sistema realizará todas las particiones necesarias en el disco duro e instalará todos los paquetes necesarios para el sistema OSSIM, que, dependiendo del perfil escogido al principio de la instalación, variarán un poco.

La configuración predeterminada de instalación de particiones en el disco duro es totalmente configurable a través de la configuración *preseed* presente en la imagen ISO de la instalación de OSSIM.

A partir de ahora, la configuración inicial del servidor y los sensores varía, por lo que vamos a tratarla en apartados diferentes.

1.1 Configuración inicial del servidor

Primero, accedemos por SSH con la dirección IP o directamente por consola al servidor e introducimos las credenciales del usuario root configuradas en la instalación del sistema OSSIM.

Lo primero que nos vamos a encontrar es la pantalla inicial con todas las opciones disponibles para configurar nuestro servidor.

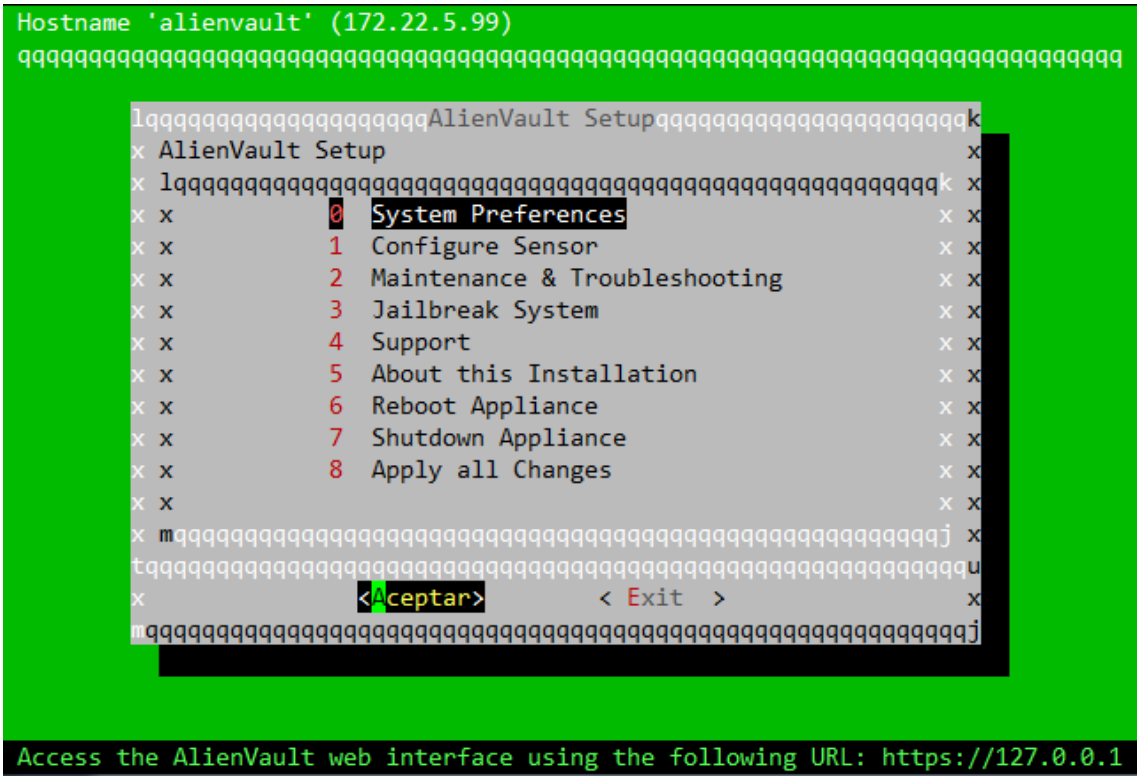


Figura 125 Configuración servidor - Pantalla inicial

Lo primero que vamos a configurar es el nombre del servidor. Para eso, accedemos a:

System Preferences > Configure Hostname

Introducimos el nombre de la máquina

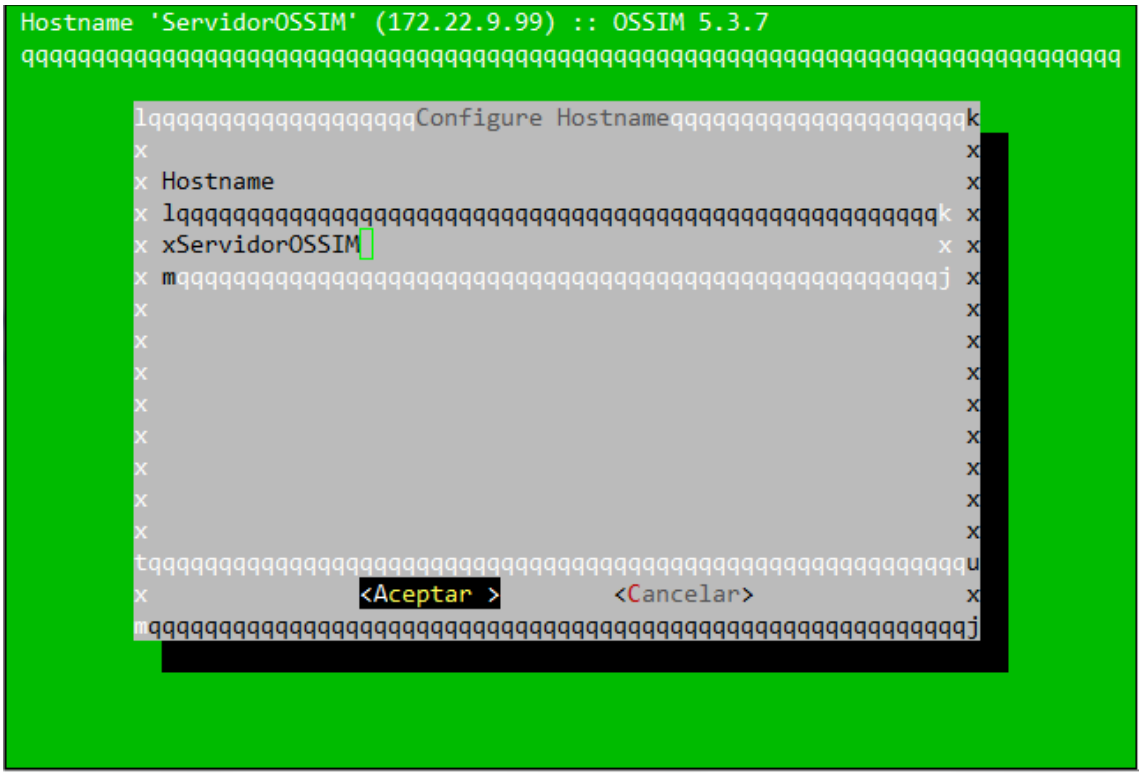


Figura 126 Configuración servidor - Nombre del servidor

Lo siguiente que haremos será configurar la direccion IP de la página web para que el servidor conceda acceso a través de dicha direcciones que en nuestro caso, será la dirección IP del servidor.

Para configurar las direcciones IP, accedemos a

Configure Sensor > Configure AlienVault Framework IP

Introducimos la dirección IP.

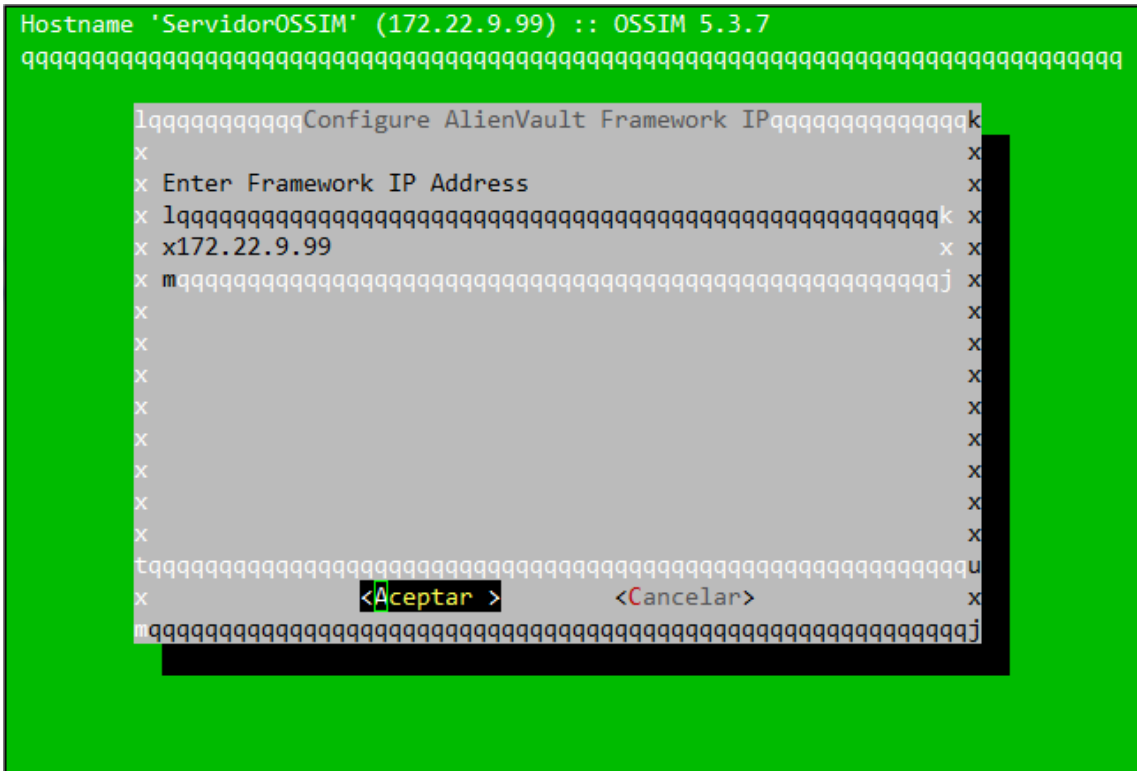


Figura 127 Configuración servidor - Introducción de dirección IP de la página web

Una vez hecho esto, el servidor está preparado para recibir todos los logs de diferentes sensores, equipos de red, software de terceros, etc.

Ahora debemos guardar los cambios y reiniciar el servidor, para eso, desde el menú principal, accedemos a

Apply All Changes

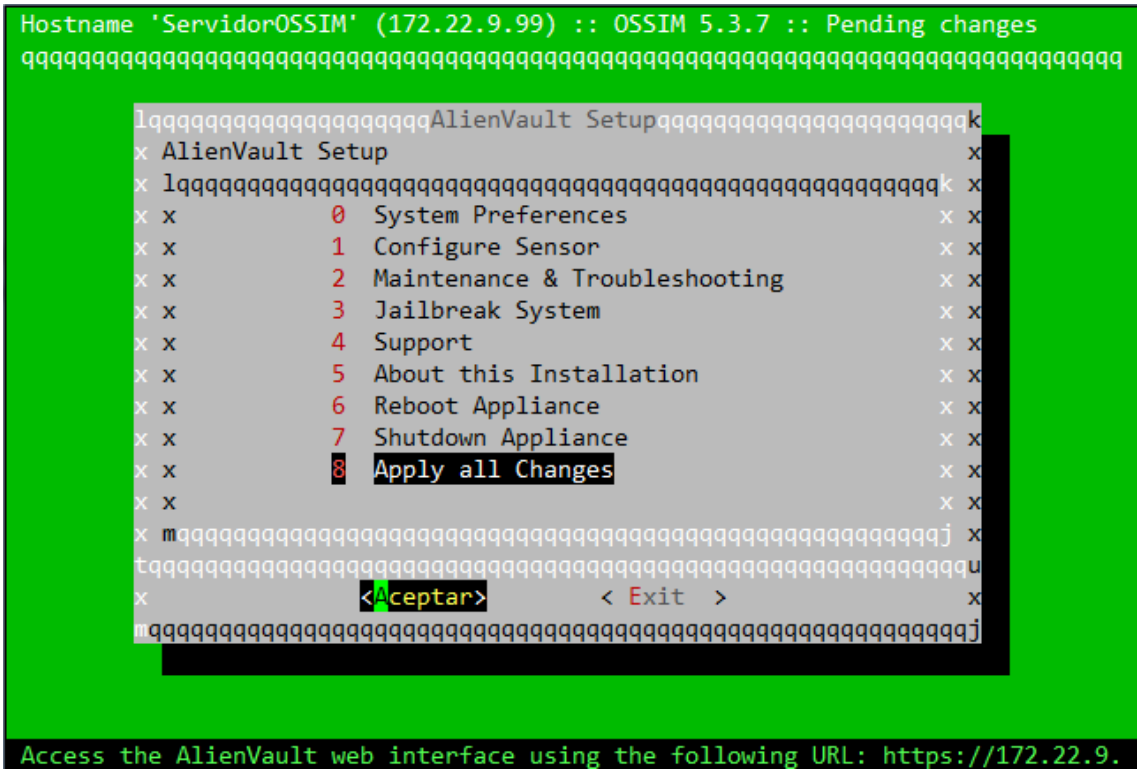


Figura 128 Configuración servidor - Guardar los cambios

Para verificar que el servidor funciona correctamente, accedemos mediante un navegador web a la dirección IP del servidor mediante HTTPS.

1.2 Configuración inicial del sensor

Lo primero que debemos hacer antes de configurar por primera vez un sensor es entrar por HTTP al servidor y acceder a

Configuration > Deployment > Components > Sensors

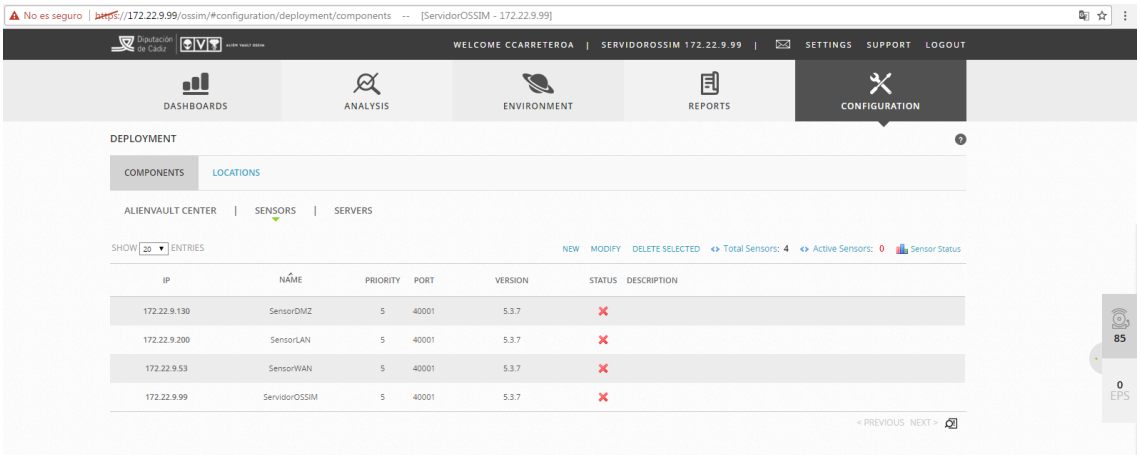


Figura 129 Configuración sensor - Sensores en la interfaz web del servidor

Debemos dejar esta pestaña del navegador abierta, puesto que una vez que el sensor se intente comunicar con el sensor por primera vez, nos aparecerá un mensaje y debemos aceptar la conexión del nuevo sensor desde la interfaz web.

Ahora, accedemos por SSH con la dirección IP o directamente por consola al sensor e introducimos las credenciales del usuario root configuradas en la instalación del sistema OSSIM.

La pantalla que nos encontramos en primera instancia es exactamente igual a la encontrada cuando accedimos anteriormente al servidor.

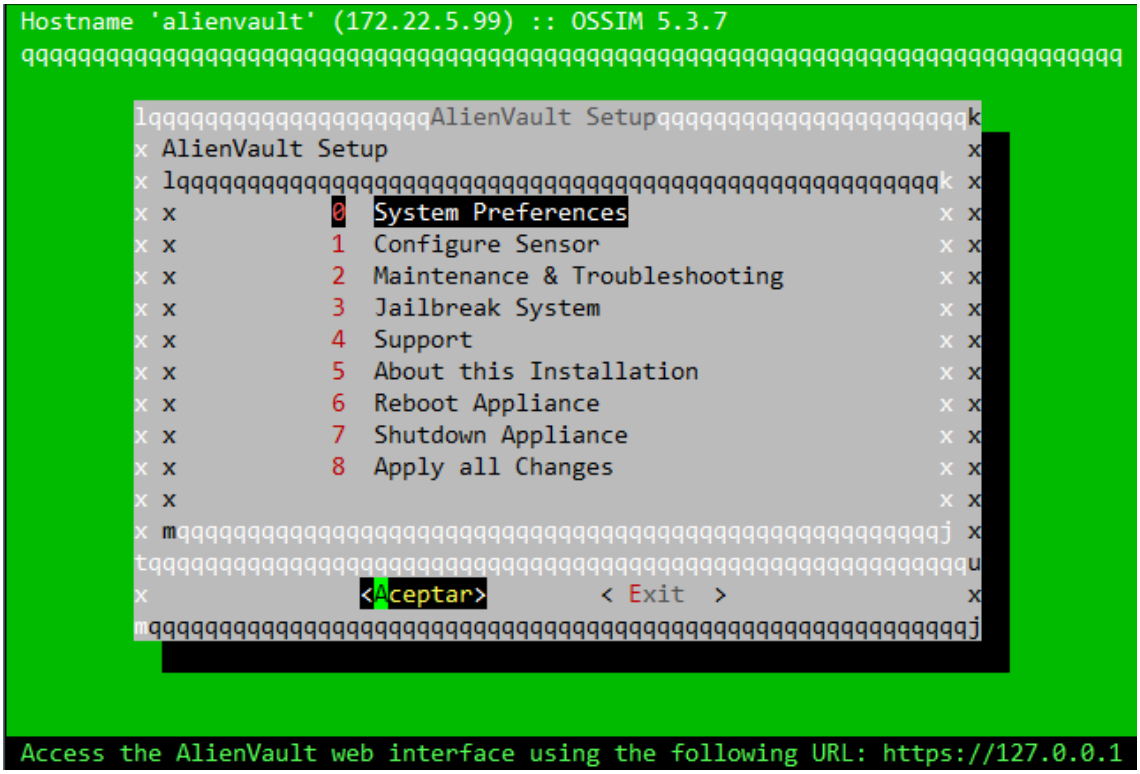


Figura 130 Configuración sensor - Pantalla inicial

Nótese el mensaje en la parte inferior que nos indica que para acceder a la interfaz web del servidor, debemos acceder a la dirección IP 127.0.0.1. Este mensaje se sustituirá por la dirección IP del servidor una vez que la configuremos. Para ello, accedemos a

Configure Sensor > Configure AlienVault Server IP

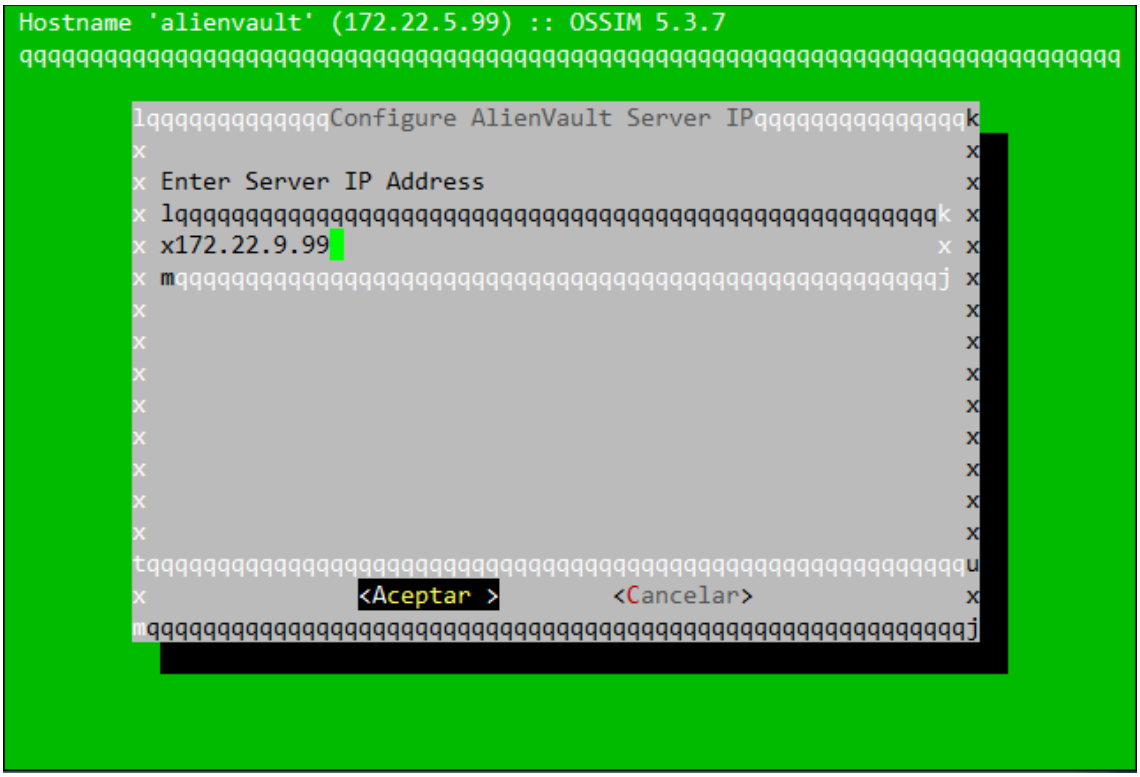


Figura 131 Configuración sensor - Configuración dirección IP del servidor

También debemos indicarle la dirección IP del framework de OSSIM que, en nuestro caso, es la misma que la dirección IP del servidor. Para ello, accedemos a

Configure Sensor > Configure AlienVault Framework IP

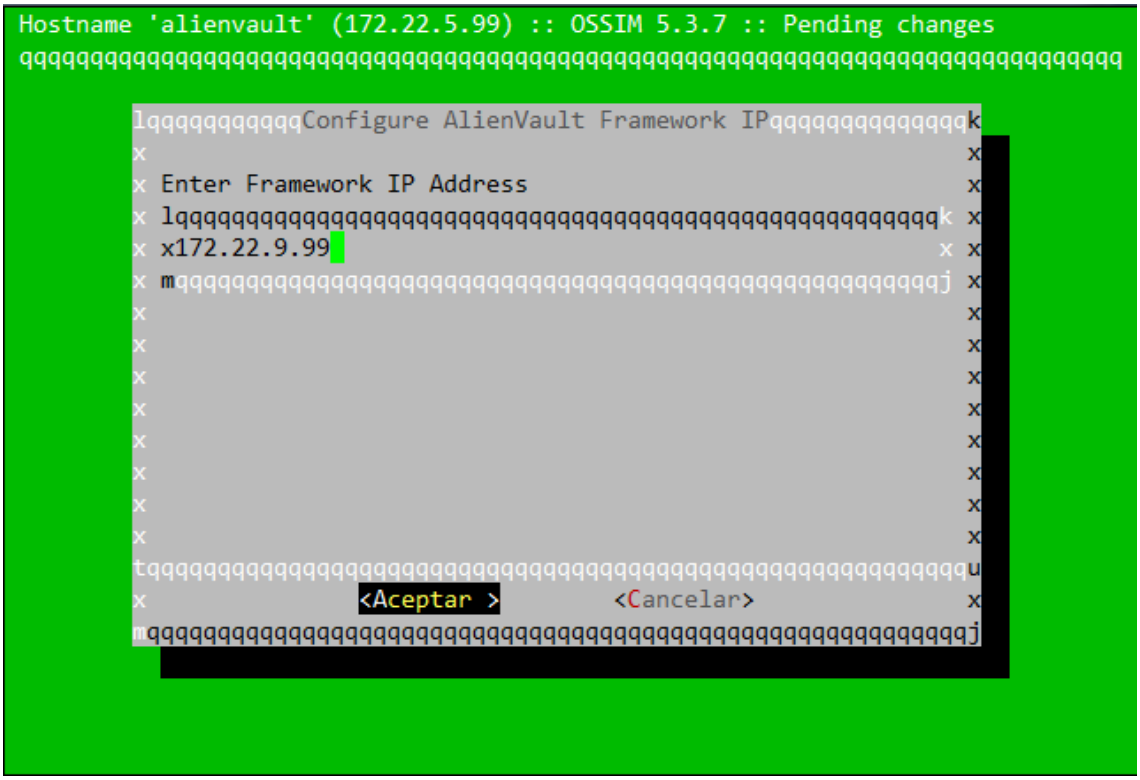


Figura 132 Configuración sensor - Configuración dirección IP del framework OSSIM

Una vez que hemos configurado la dirección donde el sensor deberá reportar toda la información relacionada con la seguridad de la red, debemos configurar la monitorización de la red.

Primero, debemos configurar la interfaz que deberá monitorizar la red. Para ello, accedemos a

Configure Sensor > Configure Network Monitoring

Debemos seleccionar la interfaz o las interfaces que deseamos que reciban todo el tráfico de red. Por defecto, OSSIM configurará esas interfaces en modo promiscuo y sin dirección IP.

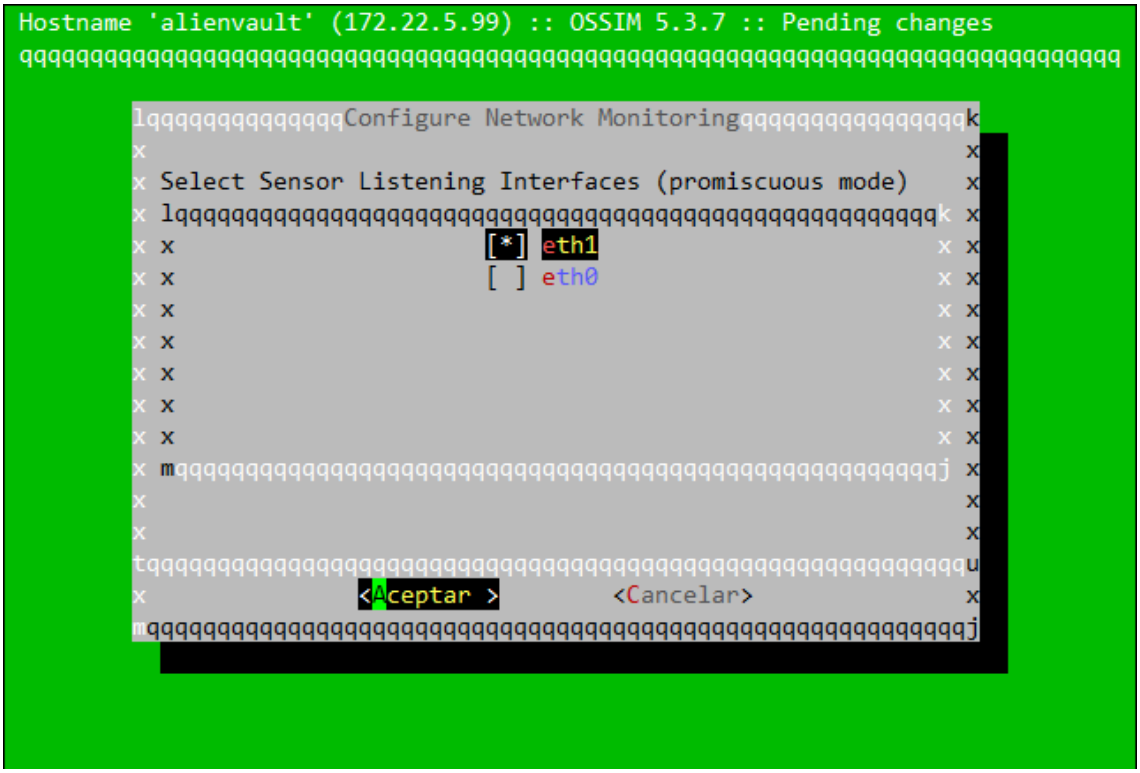


Figura 133 Configuración sensor - Configuración de la interfaz de monitorización

Ahora, debemos configurar la red que el sensor debe interpretar como red local. Debemos introducir el bloque o los bloques de direcciones IP de la red a monitorizar. Para ello, accedemos a

Configure Sensor > Network CIDRs

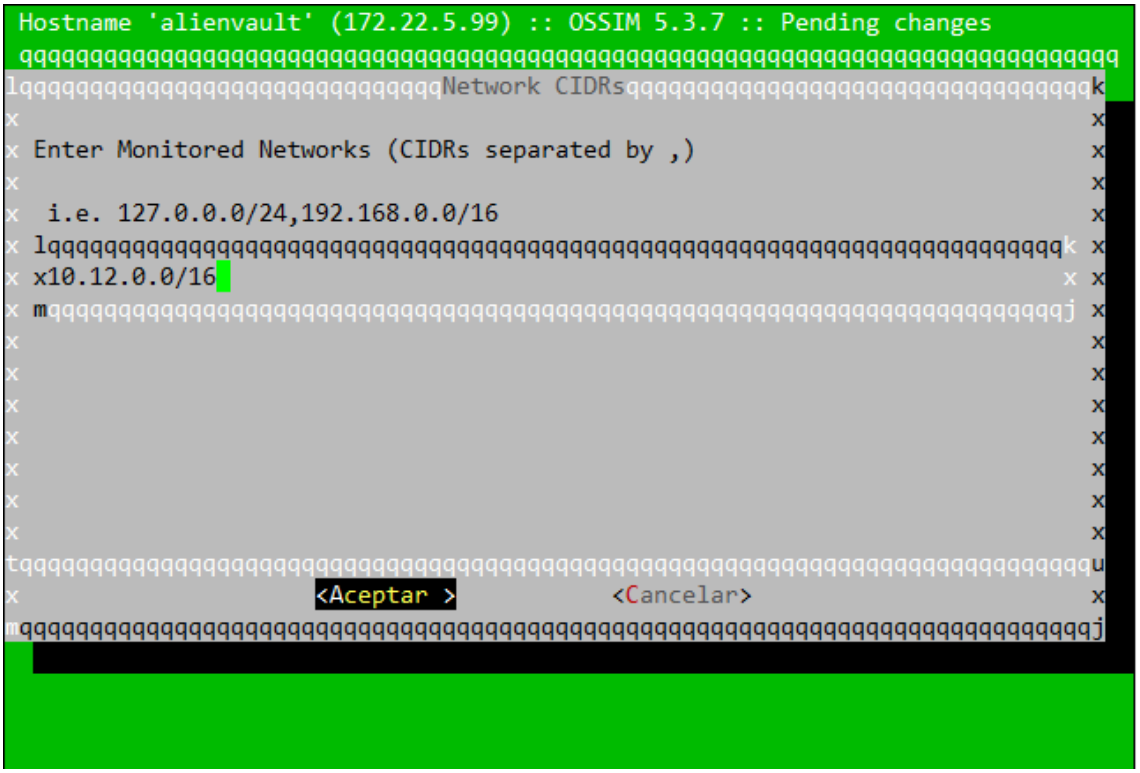


Figura 134 Configuración sensor - Configuración de red local

Por defecto, OSSIM activa la detección de intrusiones en red en el sensor y todos el software necesario para comunicarse con el servidor, por lo tanto, lo único que debemos hacer para finalizar la configuración inicial del sensor es guardar los cambios en

Apply Changes

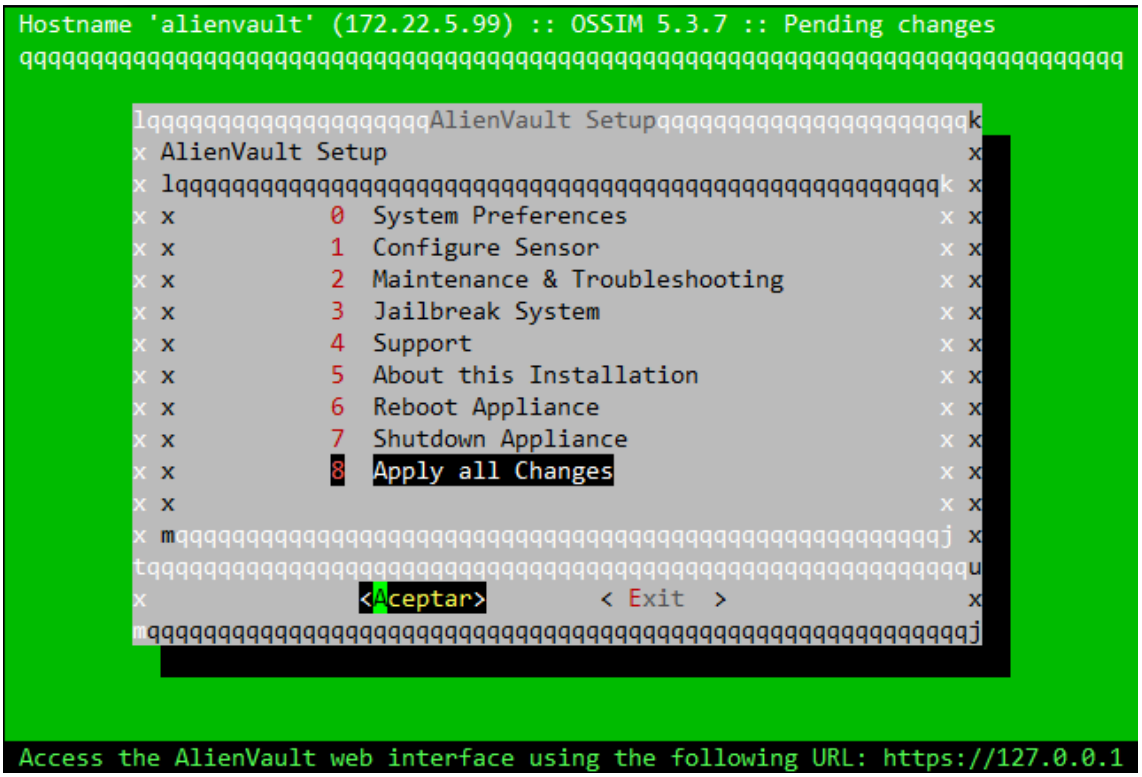


Figura 135 Configuración sensor - Guardar cambios

Si hemos configurado correctamente el sensor, deberíamos ver en la consola de administración que el mensaje de acceso al servidor ha cambiado y ya aparece la dirección IP correcta del servidor

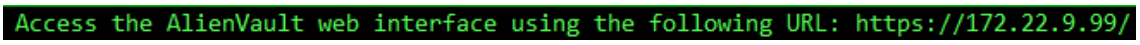


Figura 136 Configuración sensor - Mensaje de conexión al servidor correcto

Ahora, en la interfaz web del servidor debería aparecernos el siguiente mensaje

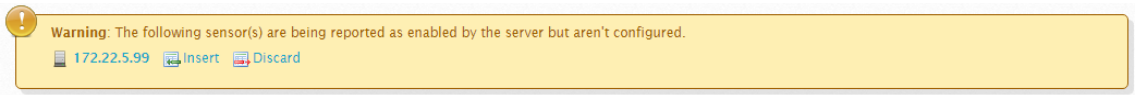


Figura 137 Configuración sensor - Mensaje de inclusión de sensor en el servidor

Lo último que debemos hacer es pulsar el botón de Insert e introducir la contraseña del usuario root del sensor, que será la que configuramos en la instalación del sistema OSSIM de dicho sensor.

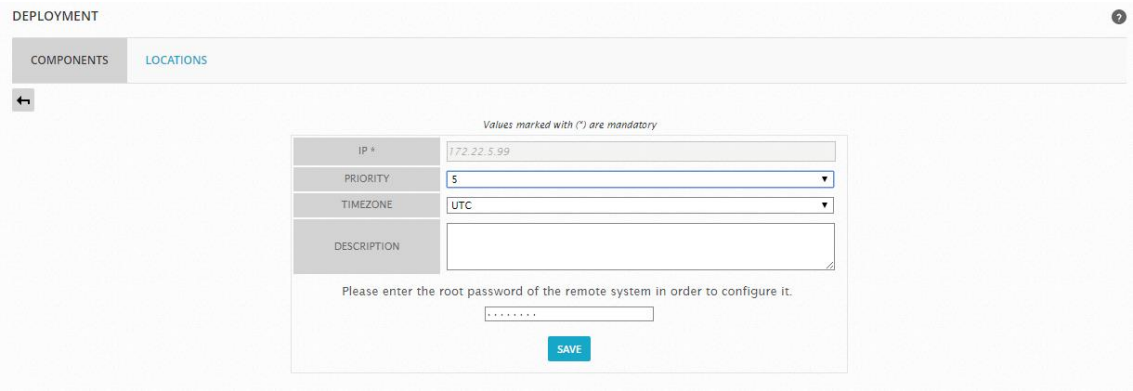


Figura 138 Configuración sensor - Inclusión del sensor desde la interfaz web del servidor

Ahora ya podemos comprobar que el sensor se ha introducido correctamente en el sistema OSSIM.

Figura 139 Configuración sensor - Comprobación de sensor en la interfaz web

2 Actualización del sistema

Para actualizar el sistema OSSIM, tanto en el servidor como en los sensores desplegados en la red corporativa, tenemos dos opciones:

- A través de la interfaz web.
- A través de una conexión remota.

2.1 Interfaz web

Para actualizar los sistemas OSSIM a través de la interfaz web, debemos entrar en la interfaz web del servidor y acceder a:

Configuration > Deployment.

Desde esta sección de la interfaz veremos si hay actualizaciones disponibles para cada uno de nuestros componentes del sistema OSSIM, ya sea el servidor o los sensores. En caso de haber actualización, nos aparecerá con un icono, el cual nos permitirá acceder a la aplicación de la correspondiente actualización.

Figura 140 Actualización web - Icono de aviso de nueva actualización

Una vez dentro de la sección de la actualización del componente deseado, debemos seleccionar si queremos actualizar solo las firmas de la detección de intrusiones o todo el software (firmas incluidas).

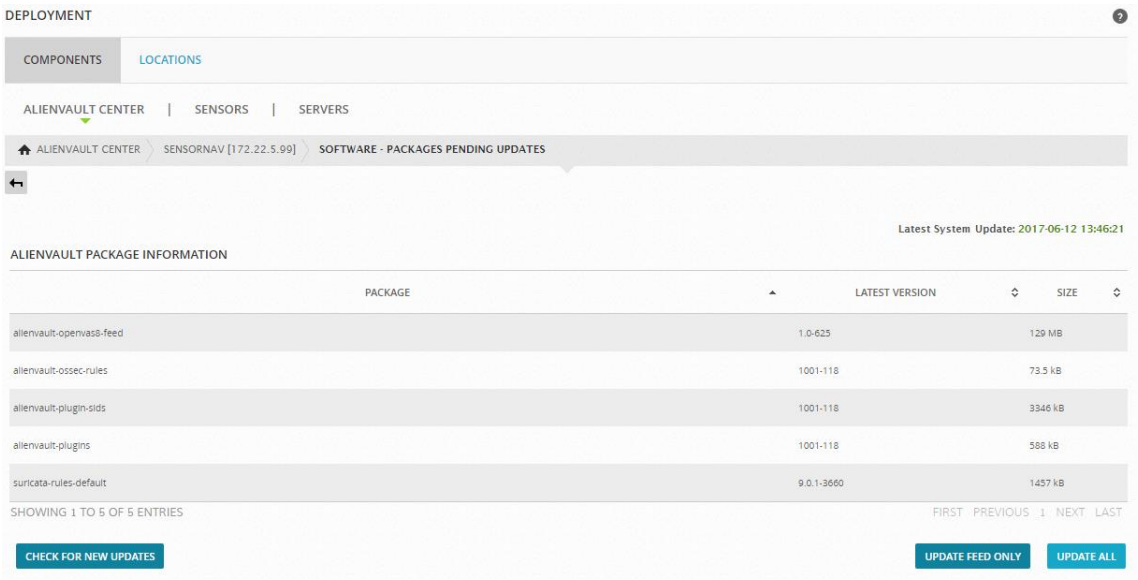


Figura 141 Actualización web - Información de actualizaciones disponibles

Seleccionamos la opción deseada y esperamos a que el sistema termine de actualizarse. Una vez que termine la actualización, el icono de aviso desaparecerá de la página de listado de componentes del sistema OSSIM.

2.2 Conexión remota

El segundo método de actualización se realiza mediante una conexión remota al sistema a actualizar mediante SSH.

Primero, accedemos al componente OSSIM que deseamos actualizar, en este caso, el sensor *SensorNAV* con dirección IP *172.22.5.99*. Introducimos las credenciales y accederemos a la sección principal de administración.

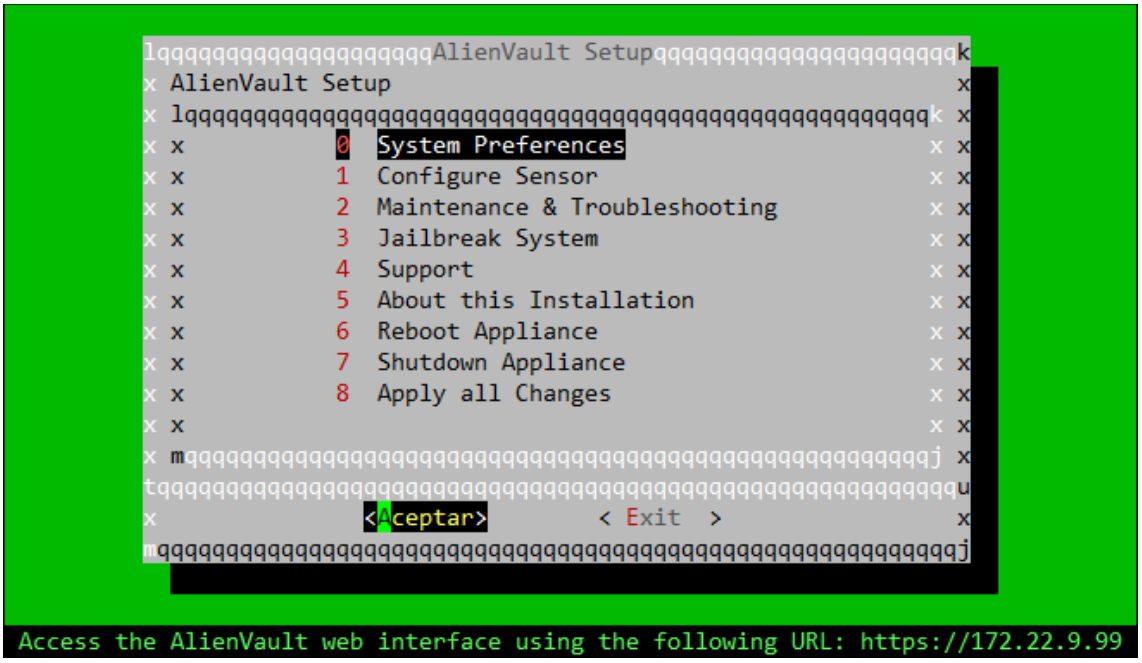


Figura 142 Actualización remota - Sección principal

Para visualiza la sección de la actualización del sistema, debemos acceder a:

System Preferences > Update AlienVault System

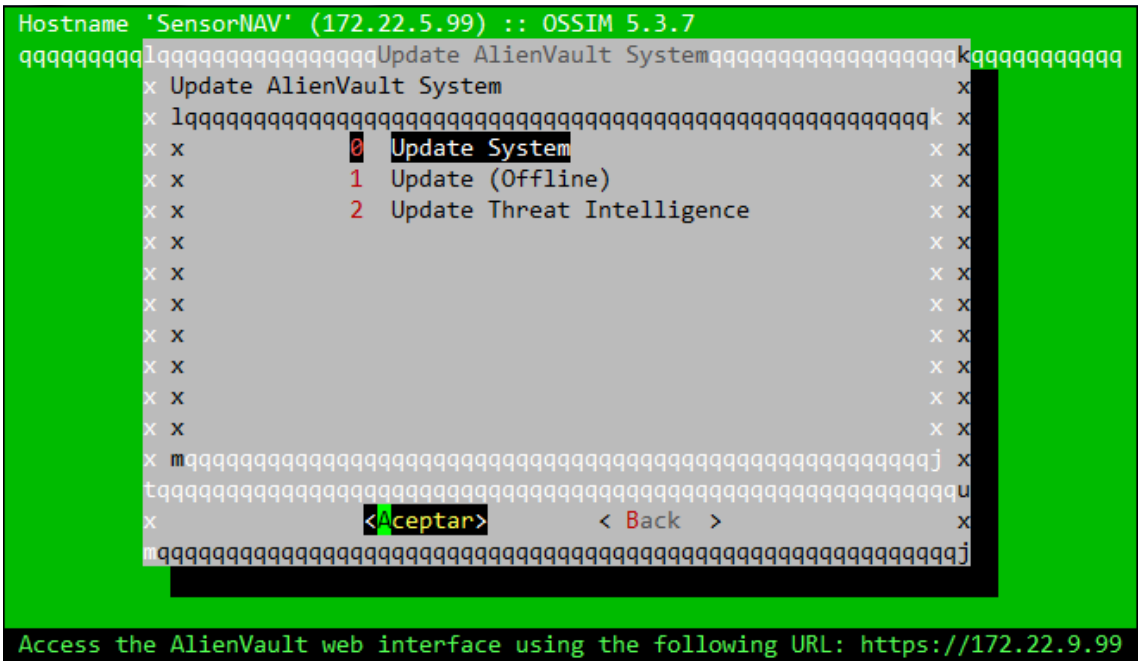


Figura 143 Actualización remota - Sección de actualización del sistema OSSIM

Desde esta sección de actualización del sistema OSSIM se ofrecen tres opciones:

0. Actualización de todo el software OSSIM y firmas a través de Internet.
1. Actualización de todo el software OSSIM y firmas a través de USB.
2. Actualización de firmas a través de Internet.

Seleccionamos la opción deseada y esperamos a que finalice la actualización.

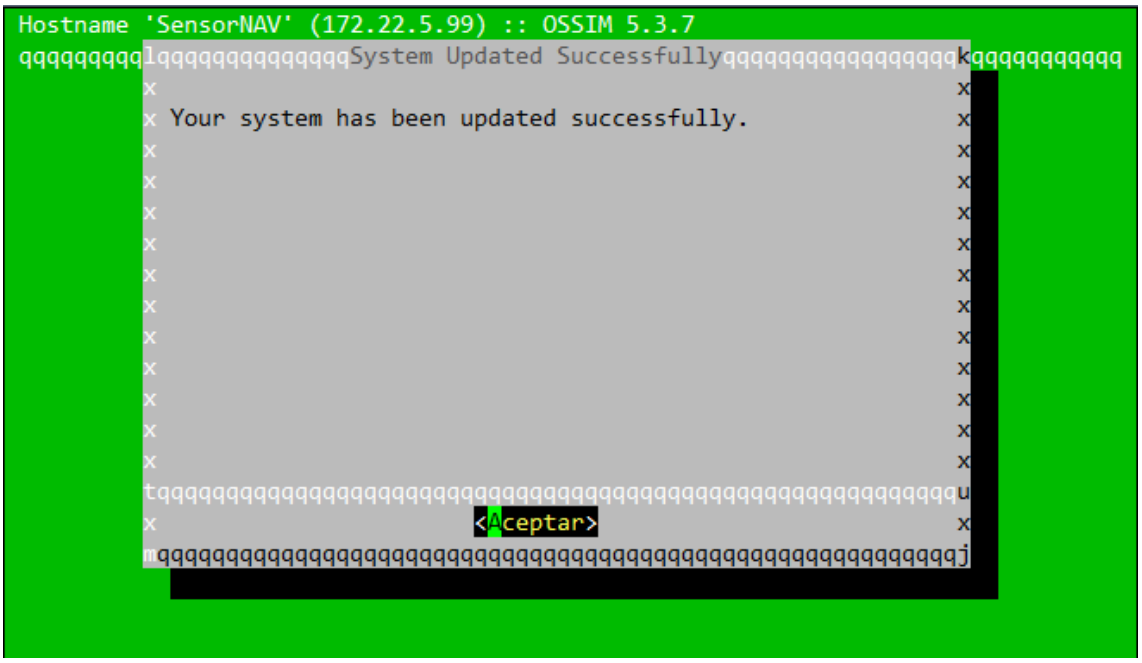


Figura 144 Actualización remota - Finalización de la actualización

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

REF: 0000001

ESPECIFICACIONES DEL SISTEMA

CLIENTE: EMPRESA PROVINCIAL DE INFORMACIÓN DE CÁDIZ S.A. (EPICSA)
PLAZA MADRID S/N, EDIFICIO CARRANZA, FONDO SUR, LOCAL 10, 11010 CÁDIZ
956261500

AUTOR: CARLOS CARRETERO AGUILAR
INGENIERO INFORMÁTICO
25603515-F
CARLOS.CARRETEROAGUILAR@ALUM.UCA.ES

FIRMADO:
SOLICITANTE AUTOR

CÁDIZ, A 1 DE JULIO DE 2017

1 Objetivos del sistema

Los objetivos del Sistema de Información de Seguridad y Administración de Eventos (SIEM) que se va a implantar en la red de la Diputación de Cádiz son los siguientes:

OBJ-01	Alertas de seguridad en red
Descripción	El sistema debe alertar cuando detecte tráfico de red sospechoso y/o indicativo de un ataque informático en la zona frontera de la red

Tabla 27 Objetivo del sistema 01

OBJ-02	Alertas de seguridad en activos
Descripción	El sistema debe alertar cuando detecte un virus o algún tipo de malware en un activo de la red

Tabla 28 Objetivo del sistema 02

OBJ-03	Inventario de activos
Descripción	El sistema debe proveer de un inventario de los activos de la red

Tabla 29 Objetivo del sistema 03

OBJ-04	Análisis de vulnerabilidades
Descripción	El sistema debe analizar las posibles vulnerabilidades presentes en los activos de la red e informar sobre las vulnerabilidades encontradas

Tabla 30 Objetivo del sistema 04

OBJ-05	Estadísticas de uso de la red
Descripción	El sistema debe analizar el uso de la red y poseer estadísticas sobre las sesiones establecidas.

Tabla 31 Objetivo del sistema 05

OBJ-06	Generación de reportes
Descripción	El sistema debe ofrecer la capacidad de generar diferentes tipos de reportes sobre alertas de seguridad generadas en la red

Tabla 32 Objetivo del sistema 06

OBJ-07	Sistema de copias de seguridad
Descripción	El sistema debe realizar copias de seguridad de todos los registros almacenados en el sistema

Tabla 33 Objetivo del sistema 07

OBJ-08	Sistema de gestión de usuarios
Descripción	El sistema debe poseer un sistema jerárquico de administración de usuarios

Tabla 34 Objetivo del sistema 08

OBJ-09	Sistema de políticas
Descripción	El sistema debe poseer un sistema de políticas para el filtrado de eventos de seguridad

Tabla 35 Objetivo del sistema 09

OBJ-10	Motor de correlación
Descripción	El sistema debe poseer un motor de correlación para los eventos de seguridad

Tabla 36 Objetivo del sistema 10

OBJ-11	Almacenamiento de larga duración
Descripción	El sistema debe almacenar durante un largo periodo de tiempo todos los eventos detectados.

Tabla 37 Objetivo del sistema 11

2 Requisitos del sistema

- **R-01**: Debe proporcionar información sobre alertas de seguridad producidas en la zona frontera de la red interna de la Diputación de Cádiz.
- **R-02**: Debe proporcionar información sobre las vulnerabilidades de los activos de la red.
- **R-03**: Debe proporcionar información sobre alertas de seguridad producidas en los equipos con sistema operativo Windows de la Diputación de Cádiz.
- **R-04**: Debe proporcionar información administrativa de la red de datos (listado de activos, estadísticas de uso, etc.).
- **R-05**: Debe definir niveles de importancia para los activos de la empresa.
- **R-06**: Debe permitir el acceso simultáneo de diferentes usuarios administradores.
- **R-07**: Debe permitir el almacenamiento prolongado de los registros.
- **R-08**: Debe tener un sistema de copias de seguridad de los registros.

Analizando la entrevista realizada con Manuel Añón Rodríguez, coordinador del departamento de redes y telecomunicaciones de la Empresa Provincial de Información de Cádiz S.A. (EPICSA), se definen los siguientes requisitos del Sistema de Información de Seguridad y Administración de Eventos que se va a implantar en la red de la Diputación Provincial de Cádiz.

R-01	**Alertas de seguridad sobre tráfico de red malicioso**
Descripción	El sistema debe alertar cuando detecte tráfico de red sospechoso y/o indicativo de un posible ataque informático
Datos asociados	- Socket de origen del tráfico. - Socket destino del tráfico. - Fecha de creación del registro. - Tipo del posible ataque. - Información del paquete que genera la alerta de seguridad.

Tabla 38 Requisito del sistema 01

R-02	**Alertas de vulnerabilidades sobre activos de la empresa**
Descripción	El sistema debe alertar cuando detecte vulnerabilidades en los activos de la empresa
Datos asociados	- Activo involucrado en la detección. - Descripción de la vulnerabilidad. - Solución de la vulnerabilidad (si existe).

Tabla 39 Requisito del sistema 02

R-03	**Alertas de seguridad en equipos Windows**
Descripción	El sistema debe alertar cuando detecte actividad sospechosa en los equipos de la Diputación de Cádiz con sistema operativo Windows
Datos asociados	- Equipo detectado. - Descripción de la actividad sospechosa. - Fecha de detección de la actividad.

Tabla 40 Requisito del sistema 03

R-04	**Información administrativa de la red**
Descripción	El sistema debe proporcionar información administrativa de la red de

	datos de la Diputación de Cádiz
Datos asociados	- Inventario de activos. - Estadísticas de uso de la red. - Información sobre las sesiones.

Tabla 41 Requisito del sistema 04

R-05	**Definición de niveles de importancia de activos**
Descripción	El sistema debe tener la capacidad de establecer niveles de importancia entre los activos de la Diputación de Cádiz.
Datos asociados	- Activo involucrado. - Nivel de importancia del activo.

Tabla 42 Requisito del sistema 05

R-06	**Acceso simultáneo de usuarios administradores**
Descripción	El sistema debe ofrecer la posibilidad de conexiones concurrentes de varios usuarios administradores, en este caso, dos como máximo
Datos asociados	- No procede

Tabla 43 Requisito del sistema 06

R-07	**Almacenamiento de registros**
Descripción	El sistema debe almacenar los registros sobre alertas de seguridad en memoria no volátil.
Datos asociados	- No procede

Tabla 44 Requisito del sistema 07

R-08	**Copias de seguridad**
Descripción	El sistema debe realizar copias de seguridad periódicas de los registros de alertas de seguridad generados en la red de la Diputación de Cádiz.
Datos asociados	- No procede

Tabla 45 Requisito del sistema 08

Si cruzamos los objetivos generales que un SIEM debe ofrecer durante su correcto funcionamiento en una red corporativa con los requisitos establecidos en la entrevista con EPICSA, se procede a la generación de una matriz de rastreabilidad de objetivos/requisitos para ver qué objetivos del sistema y qué requisitos del cliente están relacionados

	OBJ-01	**OBJ-02**	**OBJ-03**	**OBJ-04**	**OBJ-05**	**OBJ-06**	**OBJ-07**	**OBJ-08**	**OBJ-09**	**OBJ-10**	**OBJ-11**
R-01	●										
R-02				●							
R-03		●									
R-04			●		●						
R-05										●	
R-06								●			
R-07											●
R-08							●				

Tabla 46 Matriz de rastreabilidad de objetivos y requisitos

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

REF: 0000001

MEDICIONES

CLIENTE: EMPRESA PROVINCIAL DE INFORMACIÓN DE CÁDIZ S.A. (EPICSA)
PLAZA MADRID S/N, EDIFICIO CARRANZA, FONDO SUR, LOCAL 10, 11010 CÁDIZ
956261500

AUTOR: CARLOS CARRETERO AGUILAR
INGENIERO INFORMÁTICO
25603515-F
CARLOS.CARRETEROAGUILAR@ALUM.UCA.ES

FIRMADO:
SOLICITANTE AUTOR

CÁDIZ, A 1 DE JULIO DE 2017

1 Cableado

Cable	Unidades
Latiguillo RJ-45 FTP Cat. 5e LSZH (1 metro)	6
Latiguillo RJ-45 FTP Cat. 5e LSZH (5 metros)	4

Tabla 47 Mediciones de cableado

2 Equipos

Equipo	Unidades
Dell PowerEdge 2950 Server	1
HP ProLiant DL320 G5p	2
HP ProLiant DL380 G4	2

Tabla 48 Mediciones de equipos

3 Personal

Personal	Horas de trabajo
Autor del proyecto	400

Tabla 49 Mediciones de personal

4 Software

Software	Licencias
SIEM OSSIM	1

Tabla 50 Mediciones de software

IMPLANTACIÓN DE UN SISTEMA DE INFORMACIÓN DE SEGURIDAD Y ADMINISTRACIÓN DE EVENTOS EN LA RED DE LA DIPUTACIÓN DE CÁDIZ

REF: 0000001

PRESUPUESTO

CLIENTE: EMPRESA PROVINCIAL DE INFORMACIÓN DE CÁDIZ S.A. (EPICSA)
PLAZA MADRID S/N, EDIFICIO CARRANZA, FONDO SUR, LOCAL 10, 11010 CÁDIZ
956261500

AUTOR: CARLOS CARRETERO AGUILAR
INGENIERO INFORMÁTICO
25603515-F
CARLOS.CARRETEROAGUILAR@ALUM.UCA.ES

FIRMADO:
SOLICITANTE AUTOR

CÁDIZ, A 1 DE JULIO DE 2017

1 Cableado

Cable	Unidades	Precio/unidad (€)	Precio total (€)
Latiguillo RJ-45 FTP Cat. 5e LSZH (1 metro)	6	1,80	10,80
Latiguillo RJ-45 FTP Cat. 5e LSZH (5 metros)	4	2,52	10,08
		Total	**20,88**

Tabla 51 Presupuesto de cableado

2 Equipos

Equipo	Unidades	Precio/unidad (€)	Precio total (€)
Dell PowerEdge 2950 Server	1	5.680,00	5.680,00
HP ProLiant DL320 G5p	2	1.117,35	2.234,70
HP ProLiant DL380 G4	2	3.347,00	6.694,00
		Total	**14.608,70**

Tabla 52 Presupuesto de equipos

3 Personal

Personal	Horas de trabajo	Precio/hora (€)	Precio total (€)
Autor del proyecto	400	12,13	4.852,00
		Total	**4.852,00**

Tabla 53 Presupuesto de personal

4 Software

Software	Licencias	Precio/licencia (€)	Precio total (€)
SIEM OSSIM	1	0,00	0,00
		Total	**0,00**

Tabla 54 Presupuesto de software

5 Presupuesto final

	Precio (€)
Cableado	20,88
Equipos	14.608,70
Personal	4.853,00
Software	0,00
Total	**19.482,58**

Tabla 55 Presupuesto total